# REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (From - To) |
|---|---|---|
| 20-03-2016 | Final Report | 17-Sep-2009 - 16-Aug-2015 |

**4. TITLE AND SUBTITLE**
Final Report: Computer-aided Human Centric Cyber Situation Awareness

**5a. CONTRACT NUMBER**
W911NF-09-1-0525

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
611103

**6. AUTHORS**
Peng Liu, Sushil Jajodia, Massimilano Albanese, V.S. Subrahmanian, John Yen, Michael McNeese, Dave Hall, Cleotilde Gonzalez, Nancy Cooke, Douglas Reeves, Christopher Healey

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES AND ADDRESSES**
Pennsylvania State University
Office of Sponsored Programs
110 Technology Center Building
University Park, PA 16802 -7000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)**
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

**10. SPONSOR/MONITOR'S ACRONYM(S)**
ARO

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
56161-CS-MUR.182

**12. DISTRIBUTION AVAILIBILITY STATEMENT**
Approved for Public Release; Distribution Unlimited

**13. SUPPLEMENTARY NOTES**
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

**14. ABSTRACT**
In the presence of cyber warfare or cyber attacks, the security analysts need to answer four critical questions: What has happened? What is the impact? Why did it happen? What should I do? Answers to the first three questions form the core of Cyber Situational Awareness (Cyber SA). Whether the last question can be satisfactorily answered is greatly dependent upon the cyber SA capability of an enterprise.

Gaining SA is a human centric process through perception, comprehension, and projection. Compared to physical

**15. SUBJECT TERMS**
cyber situation awarenss

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 15. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Peng Liu |
| UU | UU | UU | UU | | 19b. TELEPHONE NUMBER 814-863-0641 |

## Report Title

Final Report: Computer-aided Human Centric Cyber Situation Awareness

## ABSTRACT

In the presence of cyber warfare or cyber attacks, the security analysts need to answer four critical questions: What has happened? What is the impact? Why did it happen? What should I do? Answers to the first three questions form the core of Cyber Situational Awareness (Cyber SA). Whether the last question can be satisfactorily answered is greatly dependent upon the cyber SA capability of an enterprise.

Gaining SA is a human centric process through perception, comprehension, and projection. Compared to physical world SA, cyber SA has several unique characteristics, including extremely high situation evolving speed, extremely large amount of situation information, and fully automated services. These unique characteristics imply that physical world SA techniques cannot apply in cyberspace. These unique characteristics also indicate the importance of computer-aided SA and the cognition throughput challenge in gaining cyber SA.

In this project, we take a holistic, end-to-end approach to integrate the “human cognition” aspects and the “cyber tools” aspects of cyber SA. We will develop cyber SA specific cognition models. We will leverage these models to develop cognition-friendly SA techniques, tools, and analytics, so that we can fill the gap between the sensor side and the analyst side of cyber SA. These cognition-friendly SA analytics and tools include but are not limited to situation knowledge reference model, fusion, cross-layer mission-driven SA analytics, adversary intent analysis, probabilistic graphical models, and automated reasoning. In addition, we will build test-beds to evaluate the proposed approach.

**Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:**

**(a) Papers published in peer-reviewed journals (N/A for none)**

| Received | | Paper |
|---|---|---|
| 03/17/2016 | 66.00 | Yoon-Chan Jhi, Xinran Wang, Xiaoqi Jia, Sencun Zhu, Peng Liu, Dinghao Wu. Program Characterization Using Runtime Values and Its Application to Software Plagiarism Detection, IEEE Transactions on Software Engineering, (04 2016): 0. doi: |
| 03/20/2016 | 74.00 | N. Ben-Asher, C. Gonzalez. Effects of Cyber Security Knowledge on Attack Detection, Computers in Human Behavior, (08 2015): 51. doi: |
| 03/20/2016 | 71.00 | E. Serra, S. Jajodia, A. Pugliese, A. Rullo, V.S. Subrahmanian. Pareto-Optimal Adversarial Defense of Enterprise Systems, ACM Transactions on Information & Systems Security, (11 2015): 1. doi: |
| 08/31/2012 | 45.00 | Tyworth, M., Giacobe, N.A., Mancuso, V.F., McNeese, M.D., Hall, D.L. . A Human-in-the-loop Approach to Understanding Situation Awareness in Cyber Defense Analysis, ICST Transactions on Security and Safety, (12 2012): 0. doi: |
| 08/31/2013 | 74.00 | Cooke, N. J., Champion, M., Rajivan, P., Jariwala, S. . Cyber situation awareness and teamwork , EAI Endorsed Transactions on Security and Safety, (07 2013): 1. doi: |
| 08/31/2013 | 76.00 | Dutt, V., Ahn, Y., Gonzalez, C. . Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory, Human factors, (11 2013): 0. doi: |
| 09/01/2011 | 1.00 | Shengzhi Zhang, Xiaoqi Jia, Peng Liu, Jiwu Jing. PEDA: Comprehensive Damage Assessment for Production Environment Server Systems, IEEE Transactions on Information Forensics and Security, (12 2011): 0. doi: |
| 09/01/2011 | 4.00 | Deguang Kong, Yoon-Chan Jhi, Tao Gong, Sencun Zhu, Peng Liu,, Hongsheng Xi. SAS: Semantics Aware Signature Generation for Polymorphic Worm Detection, Springer International Journal of Information Security, (11 2011): 0. doi: |
| 09/01/2011 | 3.00 | F. Li, B. Luo, P. Liu. Secure and Privacy-Preserving Information Aggregation for Smart Grids, International Journal of Security and Networks, (01 2011): 28. doi: |
| 09/01/2011 | 2.00 | J. Lin, J. Jing, P. Liu. Evaluating Intrusion Tolerant Certification Authority Systems, , (11 2011): 0. doi: |
| 09/01/2012 | 52.00 | M. Albanese, A. Pugliese, V.S. Subrahmanian. Fast Activity Detection: Indexing for Temporal Stochastic Automaton based Activity Detection, IEEE Transactions on Knowledge and Data Engineering, (12 2012): 0. doi: |
| 09/01/2012 | 63.00 | Deguang Kong, Dinghao Wu, Donghai Tian, Peng Liu. Semantic Aware Attribution Analysis of Remote Exploits, Wiley Journal of Security and Communication Networks, (12 2012): 0. doi: |
| 09/01/2012 | 62.00 | Zhi Xin, Huiyu Chen, Xinche Wang, Peng Liu, Sencun Zhu, Bing Mao, Li Xie. Replacement Attacks: Automatically Evading Behavior Based Software Birthmark, Springer International Journal of Information Security, (12 2012): 0. doi: |
| 09/01/2012 | 61.00 | Cooke, N. J., Champion, M., Rajivan, P., Jariwala, S. . Cyber Situation Awareness and Teamwork, ICST Transactions on Security and Safety, (12 2012): 0. doi: |

09/01/2014 15.00 C. Molinaro, V. Moscato, A. Picariello, A. Pugliese, A. Rullo, V.S. Subrahmanian. PADUA: A Parallel Architecture to Detect Unexplained Activities,
ACM Transactions on Internet Technology, (04 2014): 0. doi:

09/01/2014 23.00 Varun Dutt, Young-Suk Ahn, Cleotilde Gonzalez. Cyber Situation Awareness: Modeling Detection of Cyber Attacks with Instance-Based Learning Theory,
Human factors, (12 2013): 605. doi:

09/01/2014 18.00 M. Albanese, C. Molinaro, F. Persia, A. Picariello, V.S. Subrahmanian. Discovering the Top-k Unexplained Sequences in Time-Stamped Observation Data,
IEEE Transactions on Knowledge and Data Engineering, (03 2014): 577. doi:

09/01/2014 16.00 A. Pugliese, V.S. Subrahmanian, C. Thomas, C. Molinaro. PASS: A Parallel Activity-Search System,
IEEE Transactions on Knowledge & Data Engineering, (08 2014): 1989. doi:

09/02/2013 84.00 Tyworth, M., Giacobe, N.A., Mancuso, V.F., McNeese, M.D., Hall, D.L. . A human-in-the-loop approach to understanding situation awareness in cyber defence analysis,
EAI Endorsed Transactions on Security and Safety, (07 2013): 1. doi:

09/02/2013 86.00 Massimiliano Albanese, Cristian Molinaro, Fabio Persia, Antonio Picariello, V. S. Subrahmanian. Discovering the Top-k Unexplained Sequences in Time-Stamped Observation Data,
IEEE Transactions on Knowledge and Data Engineering, (12 2013): 1. doi:

09/02/2013 87.00 Lingyu Wang, Sushil Jajodia, Anoop Singhal, Pengsu Cheng, Steven Noel. k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities,
IEEE Trans. on Dependable and Secure Computing, (12 2013): 1. doi:

09/02/2013 94.00 A. Pugliese, V.S. Subrahmanian, C. Thomas, C. Molinaro. PASS: A Parallel Activity Search System,
IEEE Transactions on Knowledge and Data Engineering, (12 2013): 1. doi:

09/02/2013 98.00 Fengjun Li, Bo Luo, Peng Liu , Dongwon Lee, Chao-Hsien Chu. Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing,
IEEE Transactions on Information Forensics and Security, (02 2013): 1. doi:

09/02/2013 99.00 Xiaoqi Jia, Rui Wang, Jun Jiang, Shengzhi Zhang, Peng Liu. Defending Return Oriented Programming based on Virtualization Techniques,
Wiley Security and Communication Networks Journal, (01 2013): 1. doi:

09/02/2013 00.00 Yan Yang, Yulong Zhang, Alex Hai Wang, Meng Yu, Wanyu Zang, Peng Liu, Sushil Jajodia. Quantitative Survivability Evaluation of Three Virtual Machine based Server Architectures,
Journal of Network and Computer Applications (Elsevier), (03 2013): 1. doi:

**TOTAL: 25**

**Number of Papers published in peer-reviewed journals:**

---

## (b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

**TOTAL:**

**Number of Papers published in non peer-reviewed journals:**

## (c) Presentations

1. V.S. Subrahmanian, Invited Speaker, Israel National Cyber-Security Conference, June 2015.
2. V.S. Subrahmanian, Invited Speaker, Summer School on Business Intelligence and Big Data Analysis, Capri, Italy, June 2015.
3. V.S. Subrahmanian, Invited Speaker, Cyber-Security and Resilience Conference, Bombay Stock Exchange, Mumbai, India, April 2015.
4. V.S. Subrahmanian, Invited Participant, India-Israel Dialog, New Delhi, Dec 2014.
5. V.S. Subrahmanian, Invited Speaker, 4th Annual International Cybersecurity Conference, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli National Cyber Bureau, Prime Minister Office and the Interdisciplinary Cyber Research Center (ICRC), Sep 2014.
6. V.S. Subrahmanian, Commencement/Graduation Speaker, PES Institute of Technology, Bangalore, India, Sep 2014.
7. Cooke, N. J., Shope, S. M., Bradbury, A., & Champion, M. (2014). DEXTAR: A Cyber Security Testbed. ASU's Symposium on Information Assurance Research and Education, October 16, 2014, Tempe, AZ

**Number of Presentations:** 7.00

## Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

| Received | Paper | |
|---|---|---|
| 09/01/2012 | 49.00 | M. Albanese, S. Jajodia, A. Pugliese, V. S. Subrahmanian. Scalable Detection of Cyber Attacks, 10th International Conference on Computer Information Systems and Industrial Management Applications . 14-DEC-11, . : , |
| 09/02/2011 | 17.00 | Sushil Jajodia, Steven Noel, Pramod Kalapa, Massimiliano Albanese, John Williams. Cauldron: Mission-centric cyber situational awareness with defence in depth, MILCOM: international conference on military comm . 07-NOV-11, . : , |
| **TOTAL:** | **2** | |

**Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):**

## Peer-Reviewed Conference Proceeding publications (other than abstracts):

| Received | | Paper |
|---|---|---|
| 03/17/2016 | 49.00 | Jiang Ming, Dinghao Wu, Gaoyao Xiao, Jun Wang, Peng Liu. TaintPipe: Pipelined Symbolic Taint Analysis, USENIX Security 2015. 22-AUG-15, . : , |
| 03/17/2016 | 48.00 | Chuangang Ren, Yulong Zhang, Hui Xue, Tao Wei, Peng Liu. Towards Discovering and Understanding Task Hijacking in Android, USENIX Security 2015. 22-AUG-15, . : , |
| 03/17/2016 | 63.00 | Xiaoyan Sun, Anoop Singhal, Peng Liu. Who Touched My Mission: Towards Probabilistic Mission Impact Assessment, ACM SafeConfig Workshop 2015. 11-OCT-15, . : , |
| 03/17/2016 | 62.00 | Zhongwen Zhang, Peng Liu, Ji Xiang, Jiwu Jing, Lingguang Lei. How Your Phone Camera Can Be Used to Stealthily Spy on You: Transplantation Attacks against Android Camera Service , ACM AsiaCCS 2015. 13-APR-15, . : , |
| 03/17/2016 | 61.00 | Jun Wang, Zhiyun Qian, Zhichun Li, Zhenyu Wu, Junghwan Rhee, Xia Ning, Peng Liu, Geoff Jiang. Discover and Tame Long-running Idling Processes in Enterprise Systems, ACM AsiaCCS 2015. 14-APR-15, . : , |
| 03/17/2016 | 60.00 | Heqing Huang, Kai Chen, Chuangang Ren, Peng Liu, Sencun Zhu, Dinghao Wu . Towards Discovering and Understanding the Unexpected Hazards in Tailoring Antivirus Software for Android, ACM Asia CCS 2015. 14-APR-15, . : , |
| 03/17/2016 | 56.00 | Jun Wang, Mingyi Zhao, Qiang Zeng, Dinghao Wu, Peng Liu. Risk Assessment of Buffer 'Heartbleed' Over-read Vulnerabilities, IEEE DSN 2015. 20-JUN-15, . : , |
| 03/17/2016 | 55.00 | Bin Zhao, Peng Liu. Private Browsing Mode Not Really That Private: Dealing with Privacy Breach Caused by Browser Extensions, IEEE DSN 2015. 20-JUN-15, . : , |
| 03/17/2016 | 53.00 | Q. Zeng, M. Zhao, P. Liu. HeapTherapy: An Efficient End-to-end Solution against Heap Buffer Overflows, IEEE DSN 2015. 20-JUN-15, . : , |
| 03/17/2016 | 52.00 | C. Zhong, J. Yen, P. Liu, R. Erbacher, R. Etoty, C. Garneau. An Integrated Computer-Aided Cognitive Task Analysis Method for Tracing Cyber-Attack Analysis Processes, 2015 ACM Symposium and Bootcamp on the Science of Security. 21-APR-15, . : , |
| 03/17/2016 | 51.00 | Mingyi Zhao, Jens Grossklags, Peng Liu. An Empirical Study of Web Vulnerability Discovery Ecosystems, ACM CCS 2015. 12-OCT-15, . : , |
| 03/17/2016 | 50.00 | Kai Chen, Peng Wang, Yeonjoon Lee, Xiaofeng Wang, Nan Zhang, Heqing Huang, Wei Zou, Peng Liu. Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale, USENIX Security 2015. 22-AUG-15, . : , |
| 03/20/2016 | 75.00 | R. Wang, W. Enck, D. Reeves, X. Zhang, P. Ning, D. Xu, W. Zhou, A. Azab. EASEAndroid: Automatic Policy Analysis and Refinement for Security Enchanced Android via Large-Scale Semi-Supervised Learning, Usenix Security 2015. 20-AUG-15, . : , |

03/20/2016 70.00 M. Albanese, E. Battista, S. Jajodia. A Deception Based Approach for Defeating OS and Service Fingerprinting,
IEEE CNS 2015. 28-SEP-15, . : ,

03/20/2016 69.00 S. Venkatesan, M. Albanese, S. Jajodia. Disrupting Stealthy Botnets through Strategic Placement of Detectors,
IEEE CNS 2015. 28-SEP-15, . : ,

03/20/2016 78.00 M. Champion, S. Jariwala, P. Ward, N. J. Cooke. Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise,
Proceedings of the 58th Annual Conference of the Human Factors and Ergonomics Society. 27-OCT-14, . : ,

03/20/2016 76.00 L. Hao, C. G. Healey , S. E. Hutchinson . Ensemble Visualization for Cyber Situation Awareness of Network Security Data,
IEEE VizSec 2015. 26-OCT-15, . : ,

03/20/2016 81.00 M. D. McNeese, V. F. Mancuso, N. J. McNeese, E. Glantz. What went wrong? What can go right? A prospectus on human factors practice,
6th International Conference on Applied Human Factors and Ergonomics. 16-JUL-15, . : ,

08/31/2012 37.00 M. Ballora, Robert Cole, H. Kruesi, H. Greene, G. Mohanan, D. Hall. Use of Sonification in the Detection of Anomalous Events,
SPIE Conference on Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications. 23-APR-12, . : ,

08/31/2012 46.00 Tyworth, M., Giacobe, N.A., Mancuso, V.F. . The Distributed Nature of Cyber Situation Awareness,
Proceedings of the SPIE Conference on Defense, Security & Sensing. 23-MAR-12, . : ,

08/31/2012 42.00 Mancuso, V., McNeese, M.. Effects of Integrated and Differentiated Knowledge Structures on Distributed Team Cognition,
56th annual Meeting of Human Factors and Ergonomics Society. 22-OCT-12, . : ,

08/31/2012 40.00 Giacobe, N.A., Xu, S. . Geovisual Analytics for Cyber Security: Adopting the GeoViz Toolkit,
IEEE Symposium on Visual Analytics Science and Technology (VAST). 23-OCT-11, . : ,

08/31/2012 39.00 Mancuso, V.F., Giacobe, N.A., McNeese, M.D., Tyworth, M. . idsNETS: An Experimental Platform to Study Situation Awareness for Intrusion Detection Analysis,
IEEE Conference on Cognitive Methods in Situation Awareness and Decision Support. 04-MAR-12, . : ,

08/31/2012 38.00 Nicklaus A. Giacobe. Data Fusion in Cyber Security: First Order Entity Extraction from Common Cyber Data,
Proceedings of the SPIE Conference on Defense, Security & Sensing. 23-APR-12, . : ,

08/31/2013 72.00 Rajivan, P., Champion, M., Cooke, N. J., Jariwala, S., Dube, G., Buchanan, V. . Effects of teamwork versus group work on signal detection in cyber defense teams,
AC/HCII, LNAI 8027. 21-JUL-13, . : ,

08/31/2013 73.00 Prashanth Rajivan, Marco A. Janssen, Nancy J Cooke . Agent-based model of a cyber security defense analyst team,
Proceedings of the 57th Annual Conference of the Human Factors and Ergonomics Society. 30-SEP-13, . : ,

09/01/2011 5.00 X. Xiong, D. Tian, P. Liu. Practical Protection of Kernel Integrity for Commodity OS from Untrusted Extensions,
NDSS: Network and Distributed Systems Security. 06-FEB-11, . : ,

09/01/2011 13.00 X. Wang, X. Jia, S. Zhu, Y. C. Jhi, P. Liu, D. Wu. Value-Based Program Characterization and Its Application to Software Plagiarism Detection,
ICSE (SPIE Track): International Conference on Software Engineering . 21-MAY-11, . : ,

09/01/2011 10.00 Fengjun Li, Yuxin Chen, Bo Luo, Dongwon Lee, Peng Liu . Privacy-Preserving Group Linkage,
23rd Scientific and Statistical Database Management Conference. 20-JUL-11, . : ,

09/01/2011 9.00 J. Yu, P. Liu, Z. Li, S. Zhang. LeakProber: A framework for profiling sensitive data leakage paths,
ACM Conference on Data and Application Security and Privacy. 21-FEB-11, . : ,

09/01/2011 8.00 Deguang Kong, Donghai Tian, Peng Liu. SAEA: Automatic Semantic Aware Remote Exploits Attribution Analysis,
SECURECOMM: International Conference on Security and Privacy in Communication Networks. 07-SEP-11, . : ,

09/01/2011 7.00 Zhi Xin, Huiyu Chen, Xinche Wang, Peng Liu, Sencun Zhu, Bing Mao. Replacement Attacks on Behavior Based Software Birthmark,
ISC: The 14th Information Security Conference. 26-OCT-11, . : ,

09/01/2011 6.00 Q. Zeng, D. Wu, P. Liu. Cruiser: Concurrent Heap Buffer Overflow Monitoring Using Lock-free Data Structures,
ACM PLDI: Programming Language Design and Implementation. 04-JUN-11, . : ,

09/01/2012 50.00 M. Albanese, S. Jajodia, S. Noel. Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs,
42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012). 25-JUN-12, . : ,

09/01/2012 70.00 J. Lin, P. Liu, J. Jing. Using Signaling Games to Model the Multi-step Attack-defense Scenarios on Confidentiality,
GameSec 2012 (Conference on Decision and Game Theory for Security). 01-NOV-12, . : ,

09/01/2012 67.00 Qijun Gu, Wanyu Zang, Meng Yu, Peng Liu. Collaborative Traffic-aware Intrusion Monitoring in Multi-channel Mesh Networks,
IEEE TrustCom. 01-SEP-12, . : ,

09/01/2012 66.00 Q. Gu, K. Jones, W. Zang, M. Yu, P. Liu. Revealing Abuses of Channel Assignment Protocols in Multi-Channel Wireless Networks: An Investigation Logic Approach,
ESORICS 2012. 01-SEP-12, . : ,

09/01/2012 65.00 S. Zhang, P. Liu. Assessing the Trustworthiness of Drivers,
RAID 2012. 01-SEP-12, . : ,

09/01/2012 64.00 D. Tian, Q. Zeng, D. Wu, P. Liu, C. Z. Hu. Kruiser: Semi-synchronized Non-blocking Concurrent Kernel Heap Buffer Overflow Monitoring,
NDSS 2012. 01-FEB-12, . : ,

09/01/2012 60.00 Champion, M., Rajivan, P., Cooke, N. J., Jariwala, S. . Team-Based Cyber Defense Analysis,
2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. 06-MAR-12, . : ,

09/01/2012 59.00 Jariwala, S., Champion, M., Rajivan, P., Cooke, N. J. . Influence of team communication and coordination on the performance of teams at the iCTF competition,
56th Annual Conference of the Human Factors and Ergonomics Society. 22-OCT-12, . : ,

09/01/2012 57.00 Po-Chun Chen, Peng Liu, John Yen, Tracy Mullen. Experience-based Cyber Situation Recognition Using Relaxable Logic Patterns,
IEEE International Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2012). 06-MAR-12, . : ,

09/01/2012 55.00 N. Nazzicari, J. Almillategui, A. Stavrou, S. Jajodia. Switchwall: Automated topology fingerprinting & behavior deviation identification,
8th International Workshop on Security and Trust Management (STM 2012). 10-SEP-12, . : ,

09/01/2012 54.00 B. Peddycord III, P. Ning, S. Jajodia. On the accurate identification of network service dependencies in distributed systems,
USENIX 26th Large Installation System Administration Conference. 09-DEC-12, . : ,

09/01/2012 53.00 A. Natrajan, P. Ning, Y. Liu, S. Jajodia, S. E. Hutchinson. NSDMine: Automated discovery of network service dependencies,
INFOCOM . 25-MAR-12, . : ,

09/01/2012 51.00 M. Albanese, A. De Benedictis, S. Jajodia, P. Shakarian. A Probabilistic Framework for Localization of Attackers in MANETs,
ESORICS 2012. 10-SEP-12, . : ,

09/01/2014 10.00 L. Wang, M. Zhang, S. Jajodia, A. Singhal, M. Albanese. Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks,
the 19th European Symposium on Research in Computer Security. 07-SEP-14, . : ,

09/01/2014 47.00 Chuangang Ren, Kai Chen, Peng Liu. Droidmarking: Resilient Software Watermarking for Impeding Android Application Repackaging,
29th IEEE/ACM International Conference on Automated Software Engineering (ASE 2014). 15-SEP-14, . : ,

09/01/2014 46.00 Fangfang, Zhang, Dinghao Wu, Peng Liu, Sencun Zhu. Program Logic Based Software Plagiarism Detection,
the 25th annual International Symposium on Software Reliability Engineering. 03-NOV-14, . : ,

09/01/2014 45.00 Fangfang Zhang, Heqing Huang, Sencun Zhu, Dinghao Wu, Peng Liu. ViewDroid: Towards Obfuscation-Resilient Mobile Application Repackaging Detection,
ACM WiSec 2014. 01-JUN-14, . : ,

09/01/2014 44.00 Wenhui Hu, Damien Octeau, Patrick McDaniel, Peng Liu. Duet: Library Integrity Veri?cation for Android Applications,
ACM WiSec 2014. 01-JUN-14, . : ,

09/01/2014 43.00 Min Li, Zili Zha, Wanyu Zang, Meng Yu, Peng Liu, Kun Bai. Separating Functions from the TCB in Privacy-Preserving Virtualization,
ESORICS 2014. 01-SEP-14, . : ,

09/01/2014 42.00 Kai Chen, Peng Liu, Yingjun Zhang. Achieving Accuracy and Scalability Simultaneously in Detecting Application Clones on Android Markets,
ICSE 2014. 01-JUN-14, . : ,

09/01/2014 41.00 M. Zhao, J. Grossklags, K. Chen. An Exploratory Study of White Hat Behaviors in a Web Vulnerability Disclosure Program,
Proc. ACM WSIW Workshop, in association with CCS'14. 01-OCT-14, . : ,

09/01/2014 40.00 Lingchen Zhang, Sachin Shetty, Peng Liu, Jiwu Jing. RootkitDet: Practical End-to-End Defense against Kernel Rootkits in a Cloud Environment,
ESORICS 2014. 01-SEP-14, . : ,

09/01/2014 39.00 R. Wu, P. Chen, P. Liu, B. Mao. System Call Redirection: A Practical Approach to Meeting Real-world Virtual Machine Intropseciton Needs,
DSN 2014. 01-JUN-14, . : ,

09/01/2014 38.00 Xiaoyan Sun, Jun Dai, Anoop Singhal, Peng Liu. Inferring the Stealthy Bridges between Enterprise Network Islands in Cloud Using Cross-Layer Bayesian Networks,
SecureComm 2014. 23-SEP-14, . : ,

09/01/2014 34.00 C. Zhong, M. Zhao, G. Xiao, J. Xu. Towards Agile Cyber Analysis: Leveraging Visualization as Functions in Collaborative Visual Analytics ,
Proceedings of IEEE VAST Challenge 2013 Workshop . 01-AUG-13, . : ,

09/01/2014 33.00 C. Zhong, D. Samuel, J. Yen, P. Liu, R. Erbacher, S. Hutchinson, R. Etoty, H. Cam, W. Glodek. RankAOH: Context-driven Similarity-based Retrieval of Experiences in Cyber Analysis,
IEEE CogSIMA Conference. 01-FEB-14, . : ,

09/01/2014 31.00 S. Shaffer. Automatic theory generation from analyst text files using coherence networks,
the SPIE Conference on Sensing Technology and Applications. 01-JUN-14, . : ,

09/01/2014 29.00 J. Rimland, M. Ballora. USING VOCAL-BASED SOUNDS TO REPRESENT SENTIMENT IN COMPLEX EVENT PROCESSING,
Proceedings of the International Conference on Auditory Display. 01-JUN-14, . : ,

09/01/2014 28.00 J. Rimland, M. Ballora. Using complex event processing (CEP) and vocal synthesis techniques to improve comprehension of sonified human-centric data,
Proceedings of the SPIE Conference on Sensing Technology and Applications. 01-JUN-14, . : ,

09/01/2014 27.00 Jeff Rimland, David Hall, Steven Shaffer . A Hitchhiker's Guide to Developing Software for Hard and Soft Information Fusion,
Proceedings of the International Society of Information Fusion (ISIF) FUSION 2014. 01-JUL-14, . : ,

09/01/2014 26.00 Nicklaus A. Giacobe. A Picture is Worth a Thousand Alerts,
Proceedings of the 57th annual Meeting of Human Factors and Ergonomics Society Annual Meeting. 01-OCT-13, . : ,

09/01/2014 24.00 M. Champion, S. Jariwala, P. Ward, N. J. Cooke. Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise,
the 57th Annual Conference of the Human Factors and Ergonomics Society. 01-JAN-14, . : ,

09/01/2014 12.00 Steven Noel, Sushil Jajodia. Metrics Suite for Network Attack Graph Analytics,
9th Cyber and Information Security Research Conference. 08-APR-14, . : ,

09/01/2014 11.00 M. Albanese, E. Battista, S. Jajodia, V. Casola. Manipulating the Attacker's View of a System's Attack Surface,
2nd IEEE Conference on Communications and Network Security (IEEE CNS 2014). 29-OCT-14, . : ,

09/02/2011 15.00 M. Albanese, S. Jajodia, A. Pugliese, V.S. Subrahmanian. Scalable Analysis of Attack Scenarios,
ESORICS: European Symposium on Research in Computer Security. 12-SEP-11, . : ,

09/02/2011 31.00 N. Giacobe , S. Xu . Short Paper: Geovisual Analytics for Cyber Security: Adopting the GeoViz Toolkit,
IEEE VAST 2011. 23-OCT-11, . : ,

09/02/2011 33.00 M. Ballora, N. Giacobe, D. Hall . Songs of cyberspace: an update on sonifications of network traffic to support situational awareness,
Proc. SPIE 2011. 21-AUG-11, . : ,

09/02/2011 29.00 C. Gonzalez, V. Dutt . Instance-Based Learning Models of Training,
Proceedings of the Human Factors and Ergonomics Society 54rd Annual Meeting. 27-SEP-11, . : ,

09/02/2011 27.00 V. Dutt, Y. Ahn,, C. Gonzalez. Cyber Situation Awareness: Modeling the Security Analyst in a Cyber-Attack Scenario through Instance-Based Learning,
Proc. of DBSEC 2011 . 11-JUL-11, . : ,

09/02/2011 24.00 P. Rajivan, V. Shankaranarayanan, N. J. Cooke . CyberCog: A Synthetic Task Environment for Studies of Cyber Situation Awareness,
International Conference on Naturalistic Decision Making. 31-MAY-11, . : ,

09/02/2011 23.00 M. D. McNeese, N. J. Cooke, M. Champion. Situating Cyber Situation Awareness,
International Conference on Naturalistic Decision Making . 31-MAY-11, . : ,

09/02/2011 19.00 M. Albanese, C. Molinaro, F. Persia, A. Picariello, V.S. Subrahmanian. Finding Unexplained Activities in Video,
IJCAI: International Joint Conf. on Artificial Intelligence. 16-JUL-11, . : ,

09/02/2011 16.00 Kun Sun, Sushil Jajodia, Jason Li, Yi Cheng, Wei Tang, Anoop Singhal. Automatic security analysis using security metrics,
MILCOM: international conference for military communications. 07-NOV-11, . : ,

09/02/2013 77.00 Nicklaus A. Giacobe. A PICTURE IS WORTH A THOUSAND ALERTS ,
57th annual Meeting of Human Factors and Ergonomics Society Annual Meeting. 30-SEP-13, . : ,

09/02/2013 79.00 Giacobe, Nicklaus A., McNeese, Michael D., Mancuso Vincent F., Minotra, Dev. Capturing Human Cognition in Cyber-Security Simulations with NETS,
2013 IEEE International Conference on Intelligence and Security Informatics. 04-JUN-13, . : ,

09/02/2013 81.00 Vincent F. Mancuso, Michael D. McNeese. Effects of Integrated and Differentiated Team Knowledge Structures on Distributed Team Cognition ,
Proceedings of the 56th annual Meeting of Human Factors and Ergonomics Society Annual Meeting. 22-OCT-13, . : ,

09/02/2013 88.00 M. Albanese, S. Jajodia, A. Singhal, L. Wang. An Ef?cient Approach to Assessing the Risk of Zero-Day Vulnerabilities,
Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT 2013). 29-JUL-13, . : ,

09/02/2013 89.00 William Nzoukou Tankou, Lingyu Wang, Sushil Jajodia, Anoop Singhal. A Uni?ed Framework for Measuring a Network's Mean Time-to-Compromise,
Proc. 32nd Int'l. Symp. on Reliable Distributed Systems (SRDS). 30-SEP-13, . : ,

09/02/2013 90.00 Barry Peddycord III, Peng Ning, Sushil Jajodia. On the Accurate Identi?cation of Network Service Dependencies in Distributed Systems,
Proceedings of 26th USENIX Large Installation System Administration Conference (LISA '12). 01-DEC-12, . : ,

09/02/2013 91.00 Ruowen Wang, Peng Ning, Tao Xie, Quan Chen. MetaSymploit: Day-One Defense against Script-based Attacks with Security-Enhanced Symbolic Analysis,
Proceedings of 22nd USENIX Security Symposium (Security '13). 01-AUG-13, . : ,

09/02/2013 92.00 Lihua Hao, Christopher G. Healey, Steve E. Hutchinson. Flexible Web Visualization for Alert-Based Network Security Analytics,
VizSec 2013. 14-OCT-13, . : ,

09/02/2013 93.00 M. Ovelgonne, N. Park, V.S. Subrahmanian, L. Bowman, K. Ogaard. Personalized Best Answer Computation in Graph Databases,
2013 International Semantic Web Conference. 21-OCT-13, . : ,

09/02/2013 95.00 N. Park, M. Ovelgonne, V.S. Subrahmanian. SMAC: Subgraph Matching and Centrality in Huge Social Networks,
SOCIALCOM 2013. 08-SEP-13, . : ,

09/02/2013 01.00 M. Zhao, P. Liu. Modeling and Checking the Security of DIFC System Con?gurations,
SAFECONFIG 2012. 16-OCT-13, . : ,

09/02/2013 02.00 H. Huang, S. Zhu, P. Liu, D. Wu. A Framework for Evaluating Mobile App Repackaging Detection Algorithms,
TRUST 2013. 17-JUN-13, . : ,

09/02/2013 03.00 Jing Wang, Peng Liu, Le Guan, Jiwu Jing. Fingerprint Embedding: A Proactive Strategy of Detecting Timing Channels,
ICICS 2013. 20-NOV-13, . : ,

09/02/2013 04.00 X. Xiong, P. Liu. SILVER: Fine-grained and Transparent Protection Domain Primitives in Commodity OS Kernel,
RAID 2013. 15-OCT-13, . : ,

09/02/2013 05.00 Bin Zhao, Peng Liu. Behavior Decomposition: Aspect-level Browser Extension Clustering and Its Security Implications,
RAID 2013. 15-OCT-13, . : ,

09/02/2013 06.00 E. Yoon, P. Liu. XLRF: A Cross-Layer Intrusion Recovery Framework for Damage Assessment and Recovery Plan Generation,
ICICS 2013. 20-NOV-13, . : ,

09/02/2013 07.00 C. Zhong, D. S. Kirubakaran, J. Yen, P. Liu, S. Hutchinson, H. Cam. How to Use Experience in Cyber Analysis: An Analytical Reasoning Support System,
IEEE ISI 2013. 01-JUN-13, . : ,

09/02/2013 08.00 Jun Dai, Xiaoyan Sun, Peng Liu, Nicklaus Giacobe . Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model ,
ASE Cyber Security 2012. 14-DEC-12, . : ,

09/02/2013 09.00 Jun Dai, Xiaoyan Sun, Peng Liu. Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies,
ESORICS 2013. 01-SEP-13, . : ,

**TOTAL: 95**

**Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):**

---

## (d) Manuscripts

| Received | | Paper |
|---|---|---|
| 03/17/2016 | 67.00 | Q. Zeng, J. Rhee, H. Zhang, N. Arora, G. Jiang, P. Liu. Precise and and Scalable Calling Context Encoding, ACM Transactions on Software Engineering and Methodology (03 2016) |
| 03/17/2016 | 68.00 | C. Zhong, J. Yen, P. Liu, R. F. Erbacher. Learn from Analysts' Working Experience: Towards Automated Cybersecurity Data Triage, IEEE Transactions on Human Machine Systems (01 2016) |
| 03/20/2016 | 72.00 | L. Wang, M. Zhang, S. Jajodia, A. Singhal, M. Albanese. Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks, IEEE Transactions on Information Forensics & Security (12 2015) |
| 09/01/2011 | 11.00 | J. Lin, J. Jing, P. Liu. Using Signaling Games to Model the Multi-step Attack-defense Scenarios on Confidentiality, Submitted to NDSS 2012 (09 2011) |
| 09/01/2011 | 14.00 | Q. Gu, W. Zang, M. Yu, P. Liu. Specification-based Investigation Logic for Deterring Channel Assignment Protocol Abuses, To be submitted for publication. (09 2011) |
| 09/01/2011 | 12.00 | Jun Dai, Xiaoyan Sun, Peng Liu, Artem Balashov . Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model, Submitted to NDSS 2012 (09 2011) |
| 09/01/2012 | 58.00 | Ruowen Wang, Peng Ning, Tao Xie, Quan Chen. MetaSymploit: Lightweight Symbolic Execution of Scripting Language for Security Analysis, Submitted for publication (08 2012) |
| 09/01/2012 | 69.00 | Mingyi Zhao, Peng Liu. Modeling and Checking the Security of DIFC System Configurations, Submitted for publication (07 2012) |
| 09/01/2012 | 68.00 | Jun Dai, Xiaoyan Sun, Peng Liu, Nick Giacobe. Gaining Big Picture Awareness through an Interconnected Cross-layer Situation Knowledge Reference Model, Submitted for publication (07 2012) |
| 09/01/2014 | 17.00 | E. Serra, S. Jajodia, A. Pugliese, A. Rullo, V.S. Subrahmanian. Pareto-Optimal Adversarial Defense of Enterprise Systems, ACM Transactions on Information Systems (01 2014) |
| 09/01/2014 | 20.00 | Noam Ben-Asher, Cleotilde Gonzalez . CyberWar Game: A Paradigm for Understanding New Challenges of Cyber War , This paper has been submitted to an edited book (01 2014) |
| 09/01/2014 | 21.00 | Noam Ben-Asher, Cleotilde Gonzalez. Effects of Cyber Security Knowledge on Attack Detection, THE JOURNAL is unknown (01 2014) |
| 09/01/2014 | 25.00 | Prashanth Rajivan, Nancy J. Cooke . A Methodology for Research on the Cognitive Science of Cyber Defense , Journal of Cognitive Engineering and Decision Making (01 2014) |

09/01/2014 36.00 S. Zhang, X. Jia, P. Liu. Towards Service Continuity for Transactional Applications against Compromised Drivers,
International Journal of Information Security (07 2014)

09/01/2014 37.00 Y. Jhi, X. Jia, D. Wu, S. Zhu, P. Liu. Program Characterization Using Runtime Values and Its Application to Software Plagiarism Detection,
IEEE Transactions on Software Engineering (03 2014)

09/02/2011 18.00 M. Albanese, A. Pugliese, V.S. Subrahmanian. Fast Activity Detection: Indexing for Temporal Stochastic Automaton based Activity Detection,
Under second round review by IEEE TKDE (09 2011)

09/02/2011 20.00 Arun Natarajan, Peng Ning, Yao Liu, Sushil Jajodia, Steve E. Hutchinson. NSDMine: Automated Discovery of Network Service Dependencies,
Submitted to INFOCOM 2012 (09 2011)

09/02/2011 21.00 Nelson Nazzicari, Javier Almillategui, Angelos Stavrou, Sushil Jajodia. Switchwall: Automated Network Fingerprinting & Behavior Deviation Identification,
Submitted to INFOCOM 2012 (09 2011)

09/02/2011 22.00 Charles Bevan, Michael Young . Planning attack graphs,
Short paper submitted to ACSAC 2011 (09 2011)

09/02/2011 26.00 V. Dutt, Y. Ahn, C. Gonzalez . Cyber Situation Awareness: Modeling the Detection of Cyber Attacks with Instance-based Learning Theory,
To be submitted for publication (09 2011)

**TOTAL: 20**

**Number of Manuscripts:**

---

## Books

Received Book

08/31/2012 43.00 Ballora, M., Giacobe, N.A., McNeese, M.D., Hall, D.L. . Information Data Fusion and Computer Network Defense, Hershey PA: IGI Global, (01 2012)

08/31/2012 47.00 McMillan, E., Tyworth, M. . An Alternative Framework for Research on Situational Awareness in Computer Network Defense, Hershey, PA: IGI Global, (12 2012)

09/01/2012 56.00 David Hall. The Emergence of Human-Centric Information Fusion, Florida, USA: CRC Press, (12 2012)

09/02/2011 28.00 V. Dutt, C. Gonzalez . Cyber Situation Awareness: Modeling the Security Analyst in a cyber-attack scenario through Instance-based Learning, unknown : IGI Global, (12 2011)

09/02/2011 30.00 E. McMillan, M. Tyworth . An Alternative Framework for Research on Situational Awareness in Computer Network Defense, New York : IGI Global , (12 2011)

09/02/2011 32.00 M. Ballora, N. Giacobe, M. McNeese, D. Hall . Information Data Fusion and Computer Network Defense, New York : IGI Global , (01 2012)

**TOTAL: 6**

| Received | Book Chapter | |
|---|---|---|
| 03/17/2016 | 64.00 | X. Sun, J. Dai, A. Singhal, P. Liu. Enterprise-level Cyber Situation Awareness, Berlin New York: Springer, (12 2016) |
| 03/17/2016 | 65.00 | Chen Zhong, John Yen, Peng Liu, Rob Erbacher, Christopher Garneau. Studying Analysts Data Triage Operations in Cyber Defense Situational Analysis, Berlin New York: Springer, (12 2016) |
| 03/20/2016 | 77.00 | Christopher G. Healey, Lihua Hao, Steve E. Hutchinson. Lessons Learned: Visualizing Cyber Situation Awareness in a Network Security Domain, Berlin New York: Springer, (12 2016) |
| 03/20/2016 | 73.00 | M. Albanese, S. Jajodia. Technological Solutions for Improving Cyber Security Performance, Berlin New York: Springer, (08 2015) |
| 03/20/2016 | 79.00 | P. Rajivan, N. J. Cooke. On the Impact of Team Collaboration on Cyber SA, Berlin New York: Springer, (12 2016) |
| 08/31/2013 | 75.00 | Cleotilde Gonzalez. FromIndividualDecisionsfromExperienceto BehavioralGameTheory:Lessonsfor Cybersecurity, Germany: Springer, (07 2013) |
| 09/01/2014 | 13.00 | M. Albanese, H. Cam, S. Jajodia. Automated Cyber Situation Awareness Tools for Improving Analyst Performance, Germany: Springer, (12 2014) |
| 09/01/2014 | 32.00 | J. Yen, R. Erbacher, C. Zhong, P. Liu. Cognitive Process , Germany: Springer, (12 2014) |
| 09/01/2014 | 22.00 | Cleotilde Gonzalez, Noam Ben-Asher, Alessandro Oltramari, Christian Lebiere . Cognitive Models of Cyber Situation Awareness and Decision Making, Germany: Springer, (12 2014) |
| 09/01/2014 | 19.00 | Christopher G. Healey, Lihua Hao, Steve E. Hutchinson. Visualizations and Analysts, Germany: Springer, (12 2014) |
| 09/01/2014 | 14.00 | Massimiliano Albanese, Sushil Jajodia . Formation of Awareness, Germany: Springer, (12 2014) |
| 09/02/2013 | 85.00 | Massimiliano Albanese, Robert F. Erbacher, Sushil Jajodia, Cristian Molinaro, Fabio Persia, Antonio Picariello, Giancarlo Sperl`?, V. S. Subrahmanian. Recognizing Unexplained Behavior in Network Traf?c, Germany: Springer, (01 2014) |
| 09/02/2013 | 97.00 | Dinghao Wu, Peng Liu, Qiang Zeng, Donghai Tian. Software Cruising: A New Technology for Building Concurrent Software Monitor, Germany: Springer, (12 2013) |
| **TOTAL:** | **13** | |

## Patents Submitted

## Patents Awarded

US Patent 8,881,288, “Graphical models for cyber security analysis in enterprise networks,” by R Levy, H Li, P Liu, and M Lyell, November 4, 2014.

## Awards

Max Albanese received the 2014 George Mason University Emerging Researcher/Scholar/Creator Award.
Peng Liu received the 2015 Penn State University College of Information Sciences and Technology Faculty Excellence in Research Award.

## Graduate Students

| NAME | PERCENT_SUPPORTED | Discipline |
|---|---|---|
| Sridhar Venkatesan | 0.50 | |
| Jun Wang | 0.00 | |
| Bin Zhao | 0.00 | |
| Qiang Zeng | 0.25 | |
| P. Rajivan | 0.00 | |
| Lihua Hao | 0.50 | |
| Gaoyao Xiao | 0.50 | |
| Noseong Park | 0.50 | |
| Chanhyun Kang | 0.50 | |
| Srijan Kumar | 0.50 | |
| Ruowen Wang | 0.50 | |
| Chen Zhong | 0.50 | |
| New Entry | 0.00 | |
| Tristan Endsley | 0.50 | |
| Chuangang Ren | 0.50 | |
| Xiaoyan Sun | 0.25 | |
| Pinyao Guo | 0.25 | |
| Tao Zhang | 0.25 | |
| Eunjung Yoon | 0.25 | |
| Wenhui Hu | 0.25 | |
| **FTE Equivalent:** | **6.50** | |
| **Total Number:** | **20** | |

## Names of Post Doctorates

| NAME | PERCENT_SUPPORTED |
|---|---|
| Francesca Spezzano | 0.50 |
| Edoardo Serra | 0.50 |
| N. Ben-Asher | 0.20 |
| James Reep | 0.50 |
| Ping Chen | 0.20 |
| Le Guan | 0.10 |
| **FTE Equivalent:** | **2.00** |
| **Total Number:** | **6** |

## Names of Faculty Supported

| NAME | PERCENT_SUPPORTED | National Academy Member |
|---|---|---|
| Peng Liu | 0.16 | |
| Douglas Reeves | 0.17 | |
| Christopher Healey | 0.04 | |
| Dave Hall | 0.00 | |
| Michael McNeese | 0.00 | |
| John Yen | 0.08 | |
| Sushil Jajodia | 0.08 | |
| Massimiliano Albanese | 0.08 | |
| Nancy Cooke | 0.08 | |
| Cleotilde Gonzalez | 0.08 | |
| V.S. Subrahmanian | 0.08 | |
| **FTE Equivalent:** | **0.85** | |
| **Total Number:** | **11** | |

## Names of Under Graduate students supported

| NAME | PERCENT_SUPPORTED | Discipline |
|---|---|---|
| Daniel Jacobson | 0.20 | Information Technology |
| William Wang | 0.20 | Information Technology |
| **FTE Equivalent:** | **0.40** | |
| **Total Number:** | **2** | |

## Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: ..... 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense ..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: ..... 0.00

## Names of Personnel receiving masters degrees

| NAME | |
|---|---|
| Gaoyao Xiao | |
| **Total Number:** | **1** |

## Names of personnel receiving PHDs

| NAME |
| --- |
| Qiang Zeng |
| Jun Wang |
| Bin Zhao |
| Lihua Hao |
| P. Rajivan |
| **Total Number:** 5 |

## Names of other research staff

| NAME | PERCENT_SUPPORTED |
| --- | --- |
| **FTE Equivalent:** | |
| **Total Number:** | |

## Sub Contractors (DD882)

## Inventions (DD882)

5 **Graphical models for cyber security analysis in enterprise networks**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) N

Foreign Countries of application (5g-2):


5a: R. Levy

5f-1a: Intelligent Automation, Inc.

5f-c: 15400 Calhoun Drive

Rockville MD 20855

5a: M. Lyell

5f-1a: Intelligent Automation, Inc.

5f-c: 15400 Calhoun Drive

Rockville MD 20855

5a: P. Liu

5f-1a: Penn State University

5f-c: College of IST

University Park PA 16802

5a: H. Li

5f-1a: Intelligent Automation, Inc.

5f-c: 15400 Calhoun Drive

Rockville MD 20855


## Scientific Progress

See Attachment.

# Technology Transfer

(1)
Partner: ARL
Collaborators: Rob Erbacher, Bill Glodek, Steve Hutchinson, Hasan Cam, Renee Etoty, Chris Garneau
Effort: Collect the cognitive traces of CNDSP analysts at ARL
Accomplishment: During 2012-2015, over 30 traces have been collected; the ARSCA tool is being used offline at ARL; weekly teleconferences were held;

(2)
Partner: ARL
Collaborator: Hasan Cam
Accomplishment: Enhanced the ARL petri-net model for impact assessment.
A prototype is implemented; the first set of experiments were conducted; a set of preliminary impact assessment results are obtained.

(3)
Partner: ARL
Collaborators: Rob Erbacher, Christopher Garneau
Accomplishments: Investigated how the current practice of training professional CNDSP security analysts can be enhanced by leveraging the ARSCA toolkit developed through this MURI project. Developed a new IRB protocol and received approval. A new user study was developed. 8 human subjects conducted the designed malicious event detection task inside an fMRI scanner at Penn State University Hershey Medical Center. Through this fMRI study, the cognitive effects of different (visualization) views were investigated through brain network analysis.

(4)
Phase II STTR:
Nancy Cooke group (Arizona State University) has been working with Sushil Jajodia and Max Albanese (George Mason Univ.) on an STTR that involves a higher fidelity version of two cognitive cyber SA test-beds (i.e., CyberCog and DEXTAR) developed through this MURI project. It also involves integrating CyberCog and DEXTAR with CAULDRON which is a cyber SA toolkit developed through this MURI project.

(5)
Partner: NIST
Collaborator: Anoop Singhal
Accomplishment: Gained awareness of stealthy information bridges in a cloud; one new research work was done; a technical report is produced.

(6)
Partner: Intelligent Automation, Inc.
Collaborator: Jason Li
Accomplishment: Conducted joint R&D work on system call level enterprise cyber SA; a new U.S. patent was awarded (US Patent 8,881,288, “Graphical models for cyber security analysis in enterprise networks”).

(7)
Partner: AFRL – Human Effectiveness Directorate, 711th Human Performance Wing, Wright-Patterson AFB, OH
Collaborators: Benjamin Knott and Vince Mancuso
Accomplishment: Conducted human performance and measurement of cognition.

(8)
Partners: Deloitte, Ernst and Young, KPMG, Price Waterhouse Coopers
Collaborators: J.B. O’Kane (Vigilant by Deloitte), Jenna McAuley (EY-ASC) and others
Accomplishments: Observed practicing analysts; tested visualization toolkits and fusion tools; measured human cognition and performance

(9)
Partner: MIT Lincoln Laboratories♂Cyber Security Information Sciences Division
Collaborators: Stephen Rejto and Tony Pensa
Accomplishment: Conducted human-in-the-loop experiments; evaluate MIT-LL/PSU analyst tools.

(10)
Briefings to NSA, DTRA, ONR, and DHS.

(11)
Briefings provided to several companies including:  Deloitte, Lockheed Martin, Raytheon Corporation, MITRE, Computer

Sciences Corporation, and MIT Lincoln Laboratory.

SBIR:

Cooke group has been working on SBIR for AFRL with Charles River Associates that involves team sensors for cyber analysts.

# Scientific Progress (August 1, 2014 – July 31, 2015)

MURI: Computer-aided Human-Centric Cyber Situation Awareness

PI: Peng Liu

## Table of Content

## Scientific Progress Made by Jajodia and Albanese Group at GMU

**A Mission-centric Framework for Cyber Situational Awareness**

- **Abstract**

In the sixth year of the project – as the effort was reaching completion – the main focus was on (i) refining our overall framework for Cyber Situation Awareness; (ii) integrating the different tools and methods developed in previous years; (iii) adding new capabilities or improving existing capabilities; and (iv) summing up lessons learned over the course of the project. Specifically, we studied the problem of optimally placing detectors over a network to disrupt stealthy botnets, and we expanded our work on network diversity – which we had started in Year 5 – with the goal of modeling diversity as a security metrics and evaluating its impact on the robustness of networks against zero-day attacks.

- **Scientific Progress and Accomplishments**

Major accomplishments achieved during Year 5 include (i) a new ***probabilistic model*** to address various limitations of the previous network diversity model and metrics; (ii) a novel approach to ***optimally placing detectors*** over a network to disrupt stealthy botnets.

In Year 6, similarly to what we did in the previous 3 years, we focused on investigating in more depth specific aspects of the framework that was initially proposed in Year 1 and further refined and augmented in Year 2. The work done during Year 1 and Year 2 laid the foundations for the additional work we have done during the following years, enabling us to answer some of the fundamental questions that where defined during the first two years. Specifically, during Year 6, we focused on investigating network diversity as a security metrics and on methods for defeating stealthy botnets through optimal placement of detectors.

The framework for Cyber Situation Awareness defined during the first two years of the project envisions the capability of automatically answering a number of questions the analyst may ask about current situation, impact and evolution of an attack, behavior of the attackers, forensics, quality of available information and models, and prediction of future attacks.

In order to enable automatic tools to effectively answer these and other similar questions, it is critical to define security metrics to capture and quantify several aspects of the system being defended, such us robustness to zero-day attacks. It is also important to understand how such tools can help mitigate current and future threats, including but not limited to botnets. In the last year of the project, we focused on addressing these specific aspects.

First, building on the work we started in Year 5, we further investigated network diversity as a security property of networks. The interest in diversity as a security mechanism has recently been revived in various applications, such as Moving Target Defense (MTD), resisting worms in sensor networks, and improving the robustness of network routing. However, most existing efforts on formally modeling diversity have focused on a single system running diverse software replicas or variants. At a higher abstraction level, as a global property of the entire network, diversity and its impact on security have received limited attention. In our work, we took the first step towards formally modeling network

diversity as a security metrics for evaluating the robustness of networks against potential zero-day attacks. We have demonstrated that intuitive notions of diversity usually lead to misleading results, whereas our formal model of network diversity enables a better understanding of the impact of diversity on security. Specifically, we first devised a biodiversity-inspired metrics based on the effective number of existing distinct network resources. We then proposed two complementary diversity metrics, based on the least and the average attacking efforts, respectively. The most significant contributions since Year 5 include: (i) a ***new probabilistic model*** for addressing various limitations of the previous model; (ii) a study on ***how to instantiate the metrics***, and in particular on how to collect inputs about software diversity; and (iii) a number of different realistic ***use cases***, and a set of simulations for analyzing the proposed metrics under these different use cases. In our previous diversity model, modeling the effect of reusing exploits as a conditional probability that a resource may be exploited, given that other instances of the same type have already been exploited, essentially assumes a total order over different instances of the same resource type in any resource graph, which represents a major limitation, amongst others. Intuitively, what allows an attacker to more likely succeed in exploiting a previously exploited type of resources is the knowledge, skills, or exploit code he/she has obtained. Therefore, instead of directly modeling the casual relationship between reused exploits, we explicitly model such advantages of the attacker as separate events, and model their effect on increasing the likelihood of success in subsequent exploits as conditional probabilities.

Second, we proposed a proactive approach to strategically deploy detectors on selected network nodes, so as to either completely disrupt the communication between bots and command and control nodes (C2), or at least force the attacker to create more bots, therefore increasing the footprint of the botnet and the likelihood of detection. In our approach, we assume that the attacker can identify detector nodes, and can deploy bots in such a way to create detector-free paths through the network. However, since traffic is routed along the shortest path between source and destination, when a detector is deployed on the shortest path between a bot and a C2 site, the attacker will have to deploy additional bots to relay traffic exfiltrated by a bot to the C2 site in such a way to avoid detector nodes. In our approach, we leverage this mechanism to force the attacker to create a more complex botnet by strategically placing detectors on critical nodes. However, the problem of optimally placing detectors to monitor a network is intractable. Therefore, we proposed heuristics based on several centrality measures, and this approach enable us to identify the most promising nodes to use as detectors in a time-efficient manner. Simulations results confirm that our approach can effectively increase complexity for the attacker.

In conclusion, our efforts during Year 6 led to developing additional capabilities and further refining the framework that was defined in Year 1 and Year 2, thus achieving the objective of developing a comprehensive framework for Cyber Situation Awareness.

## Scientific Progress Made by Subrahmanian Group at UMD

- **Abstract (200 words)**

In the sixth year of this project, we continued to develop the theory, algorithms, and prototype software to support situation awareness in cyber security applications. Specifically, we looked at the following problems. (i) We developed a suite of initial forecasting models to forecast how a specific piece of malware will spread through a country and then developed an ensemble approach that takes, amongst other things, the results of the initial forecast models, and tested them on real world

data about spread of 50 types of malware from 40 countries. (ii) We looked at the problem of explaining security alerts. We have developed the novel notion of *Hyper-Graph Alert Mechanism (HAM)* and show that alert hypergraphs can be automatically extracted from known SNORT rule databases. We are developing a theoretical framework to show how a set of alerts in a real world environment can be automatically explained via the hyper-graph alert model.

- **Scientific Progress and Accomplishments**

During this year, we made one major contribution, and made a significant start on a second major contribution.

- First, we used real-world data about 1.45M hosts from around the world and 2.99M infections from the Symantec Worldwide Intelligence Network Environment (WINE) system and came up with novel new algorithms to forecast the expected number of infected machines in a country. The algorithms were tested on data about 50 different known malware and 40 countries.
- Second, we are well on the way to developing methods to automatically explain security alerts. In real world enterprises, security managers are usually swamped with the large number of alerts they receive, and any effort that helps explain what is going on is very helpful. We have developed the novel new notion of a *hypergraph alert mechanism* (or HAM) and shown how a HAM can be learned automatically from a set of SNORT rules. We then show that using sophisticated graph reachability properties, suitably modified to handle time constraints and hypergraph structure, we can generate appropriate explanation(s) of a given set of alerts that an analyst sees in front of him.

**Part 1: Country Malware Spread Forecasting**

Using the WINE data set from Symantec, we have developed an algorithm to forecast, for the first time, the expected number of hosts in a country *c* that are infected by a specific piece *m* of malware. We tested out the accuracy of our algorithms using WINE data from 40 countries and 50 different types of malware, over a population of 1.45M hosts and 2.99M malware infections.

Formally, the goal of this work is to develop methods to predict the percentage of hosts in a given population (we use country in our experiments) that will be infected by a particular piece of malware, given some historical data about the malware and the hosts, but with no information whatsoever on how the hosts are connected together. This is made even more challenging by the fact that not all truly infected machines are actually detected to be infected (by say using some anti-virus software). This problem is an important one with immediate applications in web and cyber security. For example, a better prediction of the number of infections in a country will enable anti-virus companies and security firms to better deploy patches and safety measures to counter threats.

In order to achieve this, we make several contributions.

- First, we define a very novel set of features that are related to the ability of hosts to detect malware and patch vulnerabilities. In order to achieve this, we present a novel host-malware bipartite graph and a bi-fix-point algorithm to compute these features. These lead to a feature-based prediction model (FBP).

- Then, building upon the well-known n SIR model of disease spread, we develop a custom, epidemiologically-inspired predictive model called DIPS in which each host is either in a detected, infected, patched, or susceptible state. Figure 1 shows the 4 states of each host and the possible state transitions that we can occur (as well as various parameters of the model that denote aspects of state-state transition). We define the model and show how to learn the parameters of the model in a data-driven way.

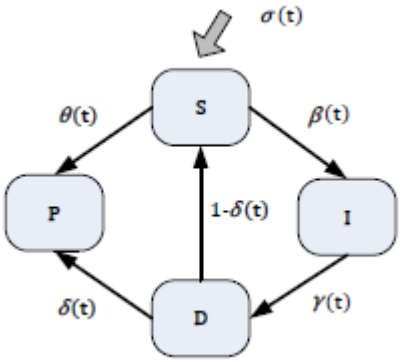



Figure 1. States and Parameters in the DIPS model

- We also define a variant of DIPS called DIPS-Exp.
- The outputs of these models, as well as outputs of past work on predicting spreads of epidemics in epidemiology, are then fed into three different ensemble models: ESM0, ESM1and FBP+Funnel. We study the relative predictive accuracies of all of these models. On split-sample 10-fold cross validation tests, ESM0 provides the best performance, significantly outperforming past work by large margins, irrespective of whether we use root mean squared error (RMSE), normalized RMSE (NRMSE), or Pearson Correlation Coefficient (PCC) as our measure. All the experiments use large-scale extensive real-data from Symantec's Worldwide Intelligence Network Environment (WINE) data set.

Our experiments answer the following questions:

**Q1**: Can we predict the number of hosts in a country that are infected by a malware?

**Q2**: How does predictive accuracy change with the number of infections?

**Q3**: Does the prediction performance of the models depend on the number of hosts monitored?

**Part 2: Hyper-graph Alert Mechanism (HAM) Framework**

A major problem in cyber-security is that a single attack or phenomenon may lead to a very large number of alerts being generated – yet, it is very difficult, often infeasible, for a security analyst to wade through a huge set of alerts and figure out exactly what events are causing them. The complexity is increased especially in the context of enterprise networks, where there are a huge number of machines connected according to a specific network topology.

In the HAM framework, we assume that SNORT rules are responsible for generating alerts. A hyper-graph alert mechanism (HAM) consists of certain types of nodes and certain specialized types of hyper-edges.

- A node is a pair *(m,a)* saying that SNORT generated alert *a* on machine *m of the enterprise network.* Note that each node is basically an alert on specific machine.
- A hyper-edge is a triple $e = (H, n, \delta)$ where
    - *H* is a set of nodes and
    - *n* is a specific node and
    - $\delta_{[e]}$ is a mapping that associates, with each $n' \in H$, a non-negative real number.

Intuitively, a hyper-edge *e* of the above form tells us that all events in *H* tend to occur more or less together, with a temporal delay between the time the events in *H* occur and the time *n* occurs. For a given event *n'* in *H*, $\delta_{[e]}(n')$ tells us the amount of time after *n'* occurred that event *n* occurs.

During this year, we first:

- Developed a formal theoretical model of hyper-edge alert mechanisms that is able to provide explanations of an alert, given a history of alerts generated in the past, not just for the current machine, but other machines as well.
- Developed an algorithm to take existing SNORT rules (especially the alert event) together with the enterprise network topology and automatically generate a set of HAMs from them.
- Implemented the above algorithm.

In addition, we started work on the following problem. Given a set of alerts $A = \{a_1, \ldots, a_k\}$ that have actually happened, what is the best explanation of this set of alerts? An explanation *E* is a set of hyper-edges with various properties. For this, we have:

- Developed a formal definition of an explanation for a given set of alerts, using the HAM structure described above;
- Define several metrics to evaluate each explanation:
    - **Hyper-Edge Size Metric.** This metric looks at the sum of the sizes of the hyper-edges (i.e. the cardinality of the sets *H* in the hyper-edges in *E*) used in the explanation.
    - **Cost Metric.** This metric is based on the cost of the explanation from the perspective of the attacker.
    - **Utility Metric.** This metric is based on the utility of the explanation (i.e. damage cost, value of information stolen) from the perspective of the attacker.

The last two metrics relate each alert with the possible software vulnerabilities causing the alerts. By using data that comes from sources such as NIST's National Vulnerability Database https://nvd.nist.gov and MITRE's Common Weakness Scoring System http://cwe.mitre.org/, it is possible to characterize each vulnerability's impact score (dangerousness of the vulnerability) and exploitability score (ease with which the vulnerability can be exploited). Thus, impact and the exploitability scores can be used as the utility and the cost of the attacker, respectively. The greater the utility (the lower is the cost), the greater is the possibility that this explanation is the right on).

- We are developing an initial algorithm able to find set of best explanations according to all different measures, by using prefixed order relation among the metrics or via Pareto optimality.
- We are developing methods able to discover new hyper-edges from the alerts logs and our HAM framework.

We expect to complete this work, including a prototype implementation, by end of 2015.

## Scientific Progress Made by Yen and Liu Joint Work at PSU

Major accomplishments achieved during the sixth year of MURI included a new approach to learn from analysts' working experience and do automated cybersecurity data triage; and an fMRI study of human analysts' brain networks in conducting cyber SA tasks.

### Learning from analysts' working experience towards automated cybersecurity data triage

Security Operations Centers (SOCs), including CNDSPs, not only employ various security measures to continuously collect network monitoring data, but also rely on security analysts to make sense of these data for attack detection and incident response. As the network monitoring data are collected at a rapid pace and may contain a lot of noise, analysts are so far bounded by tedious and repeating data triage tasks that they can hardly concentrate on in-depth analysis to generate timely and high-quality incident reports. This work aims to take the first steps towards reducing the analysts' workloads and developing data triage automatons.

**Motivation**. Many prominent companies, government organizations and military departments have spent a lot of money to construct their cyber defense system against cyber attacks. Typically, they usually set up a Security Operations Center (SOC) to do 24*7 monitoring, intrusion detection, and diagnosis (on what is actually happening). In a military setting, CNDSP (Computer Network Defense Service Provider) centers have already been established and operating for quite a few years.

SOCs usually employ multiple automated security measures, such as traffic monitors, firewalls, vulnerability scanners, Intrusion Detection/Prevention System (IDS/IPS). Besides, SOCs reply heavily on cybersecurity analysts to investigate the data from security measures to identify the true "signals" from them and "connect the dots" to answer some higher-level questions about the attack activities, for example, whether the network is under an attack; what did the attackers do; and what might be their next steps.

Although the stake of protecting an organization's mission-critical or business-critical network is already very high, organizations still run short of capabilities of detecting and reacting to the intrusions within their networks. It's because there is a huge gap between the overwhelming data from various security measures (e.g. IDS alerts) and the lack of analytics capabilities. Data analytics conducted by human analysts is important because the automated measures are in many cases unable to "comprehend" sophisticated cyber-attack strategies even through advanced correlated diagnosis. Specifically, analysts need to conduct a series of analysis, including data triage, escalation analysis, correlation analysis, threat analysis, incident response and forensic analysis. Data triage encompasses examining the details of a variety of data sources (e.g., IDS alerts, firewall logs, OS audit trails, vulnerability reports, and packet dumps), weeding out the false positives, grouping the related indicators so that different attack campaigns (i.e., attack plots) can be separated from each other. Data triage provides a basis for closer inspection in the following analysis to finally generate confidence-

bounded attack incident reports. These incident reports will serve as the primary basis for further decision-making regarding how to change current security configuration and act against the attacks.

Data triage is the most fundamental but the most time consuming stage in cyber analytics. Compared to a computer, human brains have orders of magnitudes smaller data processing throughput. In addition, human beings face unique challenges such as fatigue, anxiety and depression, which a computer would never face. However, neither the network nor the attack campaign is waiting for the human brains. The data, coming from a variety of data sources, are being continuously generated. The data volume is overwhelming. Therefore, data triage is labor-intensive and mostly performed manually by analysts.

Although SIEM (security information event management) systems take a big leap forward in generating more powerful data triage automatons, SIEM systems is extremely expensive not only for its license cost but also for the large amount of time and expertise required in constantly conducted system management and customization. Every organization needs to use a tailored SIEM system. Analysts need to develop and test the SIEM data triage automatons (e.g., customized filters and complicated correlation rules) that fit each organization's specific settings. SIEM systems involve a tremendous amount of manual effort.

**Research objective**. We aim to leverage AI techniques to dramatically reduce the cost of generating data triage automatons. We aim to automatically learn data triage automatons from analysts' working experience and data triage operation traces.

**Our new approach**.

- We leverage a computer-aided cognitive process tracing method we have developed in the second and third years of this MURI project to capture expert analysts' operations while they are performing data triage.
- We developed a 3-step approach to automatically learn data triage automatons from the traces.
    1. (Step 1) We represent the analysts' data triage operations captured in traces and their temporal and logical relationships in a newly defined Characteristic Constraint Graph (CC-Graph).
    2. (Step 2) We mine useful SIEM rule ingredients. To achieve this goal, we analyze the CC-Graphs to find the key data characteristic constraints. The key constraints are further correlated with the data sources to identify the "can-happen-before" relationships among them. The key constraints and their "can-happen-before" relationships represent various attack patterns, named "Attack Path Pattern". Each attack path pattern, which is formally represented, has a semantic meaning that defines a class of network connections indicating multi-step attacks. Analysts can review, modify and extend them.
    3. (Step 3) We directly use the formally represent attack path patterns to build a finite state machine for conducting automated data triage, just as adding rules to a SIEM system. The data triage is essentially a data triage automaton.

**Our main contributions**.

- We developed an innovative AI technique to to automatically learn data triage automatons from analysts' data triage operation traces.
- We evaluated our approach in a human-in-the-loop case study. 30 professional security analysts were recruited in the study and asked to complete a cyber-attack analysis task with

their task operations being traced. Selecting several sets of traces, rule sets were discovered from each set of traces and used to construct a set of data triage state machines. False positive and false negative rates were calculated to evaluate the performance of the state machines by comparing their data triage results with the ground truth.

- The results show that all the state machines were able to finish processing a much larger data set within several minutes. We found that the state machine built on the traces from the analysts with better task performance have a better data triage performance. Besides, the state machine built on a combination of analysts' traces has better performance than the average performance of the state machines built on individual traces.

## Studying Neural, Visual, and Cognitive Processes of Network Security Analysts Using fMRI

**Background**: Network security analysts perform a highly challenging task that is critical to cyber security: they detect malicious events from a huge influx of network security monitoring data, which includes a large amount of "false alerts". Their tasks are also highly dynamic, because strategies of attackers change over time and may even exploit new vulnerabilities that have not been exploited by previous attacks. The extremely complex and highly dynamic natures of the network security analysis task present major challenges for understanding the fine-grained cognitive processes of analysts and the impact of different visual presentation of network data on these cognitive processes and the performance of analysts. Previous works on visualization for cyber security have proposed alternative presentation of network data; however, the impacts of different visual presentation of network data to the cognitive process of network analysts remain unknown. Brain images captured by fMRI produce activation maps that show which parts of the brain are involved in a particular brain activity. However, the complexity of the cyber security analysis task presents a much higher level of challenge to the design of an fMRI study for the task.

**Goals and research questions**: The goal of this work is to obtain pilot data regarding fine-grained cognitive processes of network security analysts using fMRI and eye-tracking facility at Penn State SLEIC (Social, Life, and Engineering Sciences Imaging Center). The research questions of the experiment include the following: Does two different visualization displays (one is a conventional tabular display, the other is a novel node-link display) of network alert data result in different neuro-cognitive processes? Are there differences in the neuro-cognitive processes of subjects whose task performance differ?

**Main accomplishments**:

- We have developed an IRB-approved protocol entitled "Studying Neural, Visual, and Cognitive Processes of Network Security Analysts Using fMRI, EEG, and Eye Tracking", which has also been approved by the Army Human Research Protection Office (HRPO).
- To adapt the complexity of network security analysis task to the short time duration of each visual stimulus in an fMRI study, we have designed "network security analysis cards" that require the subject to determine whether alerts in the cards indicate malicious events. Two types of visual displays of alerts (i.e., tabular display and node-link display) are used to create two groups of analysis cards (using identical alert contents).

- We have recruited 6 subjects and they have conducted the above malicious event detection task insider an fMRI scanner located at Penn State Hershey medical center.
- We have analyzed the obtained brain image data. In particular, we have constructed brain network graphs from the obtained fMRI data. In constructing the graphs, we started with 120 ROIs (region of interests) then we followed a standard procedure to do down-selecting and we finally selected 38 features which belong to six categories (weighted clustering coefficient, Eigen centrality, betweenness, clustering coefficient, degree, and average neighbor degree).
- Using the selected 38 features, we have conducted brain network graph classification analysis to see whether two different visualization displays (one is a conventional tabular display, the other is a novel node-link display) of the same IDS alerts result in different brain images.
- We obtained a set of findings through the above classification analysis.

The aforementioned research accomplishments are the result of a multi-year collaboration process with ARL researchers. Through the 12 months, weekly teleconferences had been held on every Thursday from 9am to 10:20am. During the past 12 months, Prof. John Yen took two trips to visit Army Research Lab. During the visits, Prof. Yen did on-site collaborative research with Dr. Rob Erbacher in the Network Security Branch and Dr. Chris Garneau in the Human Research and Engineering Directorate. These teleconferences and trips have further strengthened the collaboration relationships with ARL researchers.

## Scientific Progress Made by Liu Group at PSU

Besides the joint work with Professor Yen, major accomplishments achieved during Year 6 include (1) Using Bayesian Networks to do evidence fusion towards detection of zero-day attack paths in enterprise networks; and (2) Discover and Tame Long-running Idling Processes in Enterprise Systems.

### Using Bayesian Networks to do evidence fusion towards detection of zero-day attack paths in enterprise networks

Since cyber SA (Situation Awareness) in large enterprise networks is gained through synthesized analysis of multiple data sources, evidence fusion is a fundamentally important cyber SA capability. In the literature, a variety of homogeneous evidence fusion techniques (e.g., alert correlation) have been developed. However, automated ***heterogeneous*** evidence fusion is a relatively unexplored research area. In practice, heterogeneous evidence fusion is primarily relying on SIEM (security information event management) rules manually developed by security analysts. Unfortunately, it is extremely expensive to generate high quality SIEM rules.

In this work, we take the first steps towards using Bayesian Networks to do evidence fusion towards detection of zero-day attack paths in enterprise networks.

***Motivation***. Detecting zero-day attacks is one of the most fundamentally challenging cyber SA problems yet to be solved. Zero-day attacks are usually enabled by unknown vulnerabilities. The information asymmetry between what the attacker knows and what the defender knows makes zero-day exploits extremely hard to detect. Signature-based detection assumes that a signature is already

extracted from detected exploits. Anomaly detection may detect zero-day exploits, but this solution has to cope with high false positive rates.

Considering the extreme difficulty of detecting individual zero-day exploits, a substantially more feasible strategy is to identify zero-day attack paths. In real world, attack campaigns are relying on a chain of attack actions, which forms an attack path. Each attack chain is a partial order of exploits and each exploit is exploiting a particular vulnerability. A zero day attack path is a multi-step attack path that includes one or more zero-day exploits. A key insight in dealing with zero-day attack paths is to analyze the chaining effect. Typically, it is not very likely for a zero-day attack chain to be 100% zero day, namely having every exploit in the chain be a zero-day exploit. Hence, defenders can assume that 1) the non-zero-day exploits in the chain are detectable; 2) these detectable exploits have certain chaining relationships with the zero-day exploits in the chain. As a result, connecting the detected non-zero-day segments through a path is an effective way of revealing the zero-day segments on the same chain.

Both alert correlation and attack graphs are possible solutions for generating potential attack paths, but they are still very limited in revealing the zero-day ones. A main reason for why they are still very limited is that they both do homogeneous evidence fusion and they both have very limited capability to do ***heterogeneous*** evidence fusion. A key observation we got is that zero-day attack path detection requires heterogeneous evidence fusion; homogeneous evidence fusion is simply not adequate.

***Main contributions***.

- We developed an innovative technique which uses Bayesian Networks to do heterogeneous evidence fusion towards detection of zero-day attack paths in enterprise networks.
- We proposed constructing Bayesian network at the system object level by introducing the object instance graph.
- We have designed, implemented and evaluated a system prototype named ZePro, which can effectively and automatically identify zero-day attack paths.

***Significance of this work.*** The significance of our approach is as follows: 1) our approach is systematic because Bayesian networks can incorporate literally all kinds of knowledge the defender has about the zero-day attack paths. The knowledge includes but is not limited to alerts generated by security sensors such as IDS and Tripwire, reports provided by vulnerability scanners, system logs, or even human inputs. 2) Our approach does not rely on particular assumptions or preconditions. Therefore, it is applicable to almost all kinds of enterprise networks. 3) Our approach is elastic. Whenever new knowledge is gained about zero-day attacks, such new knowledge can be incorporated and the effectiveness of our approach can be enhanced. Whenever erroneous knowledge is identified, our approach can easily get rid of the negative effects of the wrong knowledge. 4) The tool we built is automated. Today's security analysis relies largely on the manual work of human security analysts. Our automated tool can significantly save security analysts' time and address the human resource challenge.

## Discover and Tame Long-running Idling Processes in Enterprise Networks

Attack graphs play an essential role in gaining cyber SA in large enterprise networks; however, the vulnerability analysis results provided by attack graph analytics are actually ***incomplete***. This leads to incomplete cyber SA in terms of how vulnerable the enterprise network is.

In this work, our goal is to gain more complete cyber SA through discovering long-running idling processes in enterprise networks. In many cases, the long-running idling processes substantially enlarge the attack surface of the enterprise network, but they often do not have any known vulnerability which a scanner such as NESSUS can report to an attack graph toolkit. This is why attack graphs cannot provide situation awareness of this portion of the attack surface.

***Motivation***. Gaining awareness of the attack surface and reducing it is an effective preventive measure to strengthen security in large enterprises. However, it is challenging to apply this idea in an enterprise environment where systems are complex and evolving over time. In this work, we aim to empirically analyze and measure a real enterprise to identify unused services that expose attack surface. Interestingly, such unused services are known to exist and summarized by security best practices, yet the existing solutions require significant manual effort.

***Main contributions***.

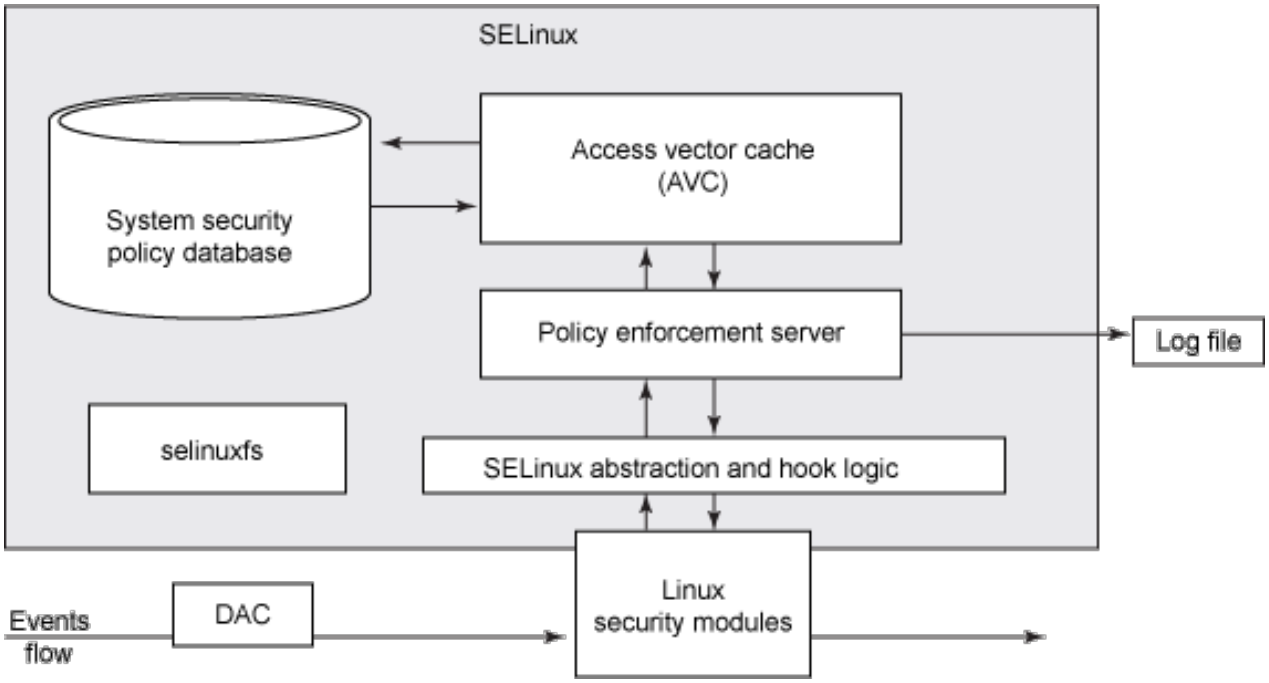
- We propose an automated approach to accurately detect the idling (most likely unused) services that are in either blocked or bookkeeping states. The idea is to identify repeating events with perfect time alignment, which is the indication of being idling.
- We implement this idea by developing a novel statistical algorithm based on autocorrelation with time information incorporated.
- From our measurement results, we find that 88.5% of the detected idling services can be constrained with a simple syscall-based policy, which confines the process behaviors within its bookkeeping states. In addition, working with two IT departments (one of which is a cross validation), we receive positive feedbacks which show that about 30.6% of such services can be safely disabled or uninstalled directly. Leveraging the new awareness, IT departments can incorporate the results to build a "smaller" OS installation image.
- We believe our discovery results raise the awareness of the potential security risks of idling services.

## Scientific Progress Made by Reeves and Healey Group at NCSU

### Automatic Policy Analysis and Refinement for Security Enhanced Android via Large-Scale Semi-Supervised Learning (From Douglas Reeves)

In this project we focus on automating / assisting those tasks that improve security for enterprises. The volume, arrival rate, and complexity of system log data, as well as the stealth of attacks, overwhelms the ability of defenders to understand and manage their security posture. We have previously worked on automated network service discovery, and automated rule creation for network intrusion detection / prevention systems. We are now concentrating on automated analysis of audit logs generated by access control systems. For a large population of users, over a period of time measured in months or years, such logs can run into many millions of entries, or greater. The intended output of such automated analysis is a security policy that can be parsed and enforced by some form of mandatory access control.

A figure illustrating MAC and its enforcement by the SELinux system is below:




*URL: http://www.ibm.com/developerworks/library/l-secure-linux-ru/figure_01-trans.gif*

Mandatory access control (MAC) has a number of advantages over discretionary access control (DAC). However, because of the difficulty of creating, understanding, optimizing, and maintaining security policies, MAC is typically turned off, or a weak, generic policy is used which is not very effective at preventing misuse. In theory, if it was possible to identify in advance every possible non-malicious access operation executed by every piece of installable software, an appropriate security policy could be derived that would permit these operations, and no more. This unfortunately is not a realistic goal.

It is, however, realistic to capture from a large population of users, over a sufficient interval of time, most of the access operations that are needed in practice, and to process this information to derive a security policy. There are several research questions that must be answered in doing so:

1. Is it possible to distinguish the operations executed by normal (non-malicious) users and software from operations executed by malicious software, intended to compromise the system or access information that should be protected?
2. Is it possible to generate automatically a security policy that allows normal accesses and prevents malicious accesses, in a way that makes the policy both human readable and efficient to enforce?
3. Will such a method scale to information captured from millions of users over extended periods of time?
4. Will the quality of the generated security policy, as judged by human analysts (security specialists), be equal to or better than the quality of manually derived security policies?

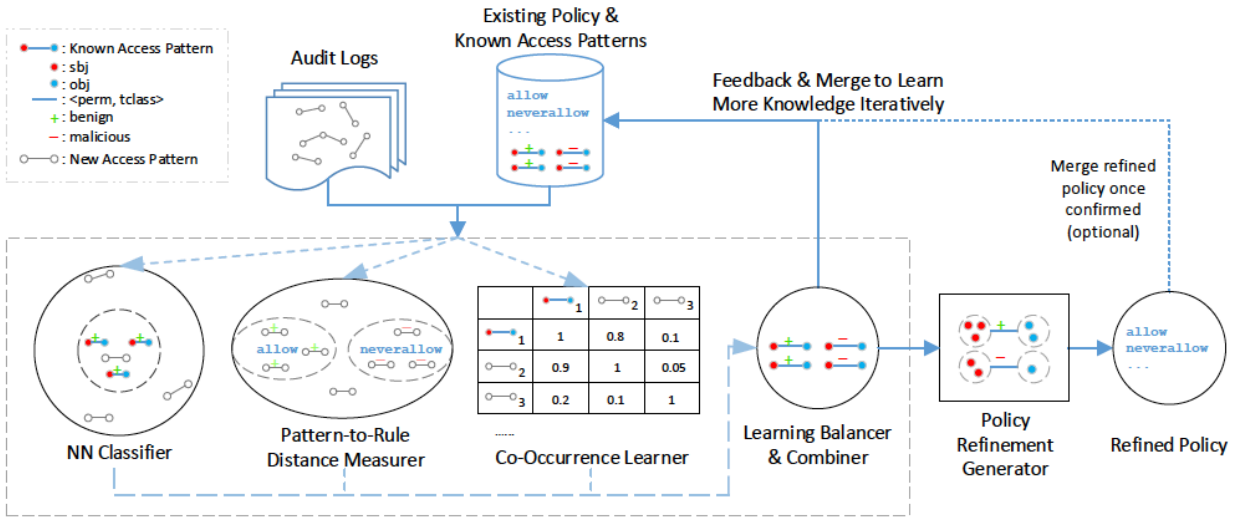
We have investigated this issue using as a demonstration system the Android smartphone, which is the most widely used computing and communication device in the world. Through a partnership with Samsung, we obtained access to a rich dataset of user access operations, collected from millions of users (with their permission). We have proposed and evaluated a method of automatically creating security

policies which can be enforced by the MAC layer (SEAndroid) of Android devices. This approach answers the above research questions in the affirmative, with some limitations. We believe the technique is usable for any platform, and any MAC system, for which a large and diverse corpus of user access operations can be collected.

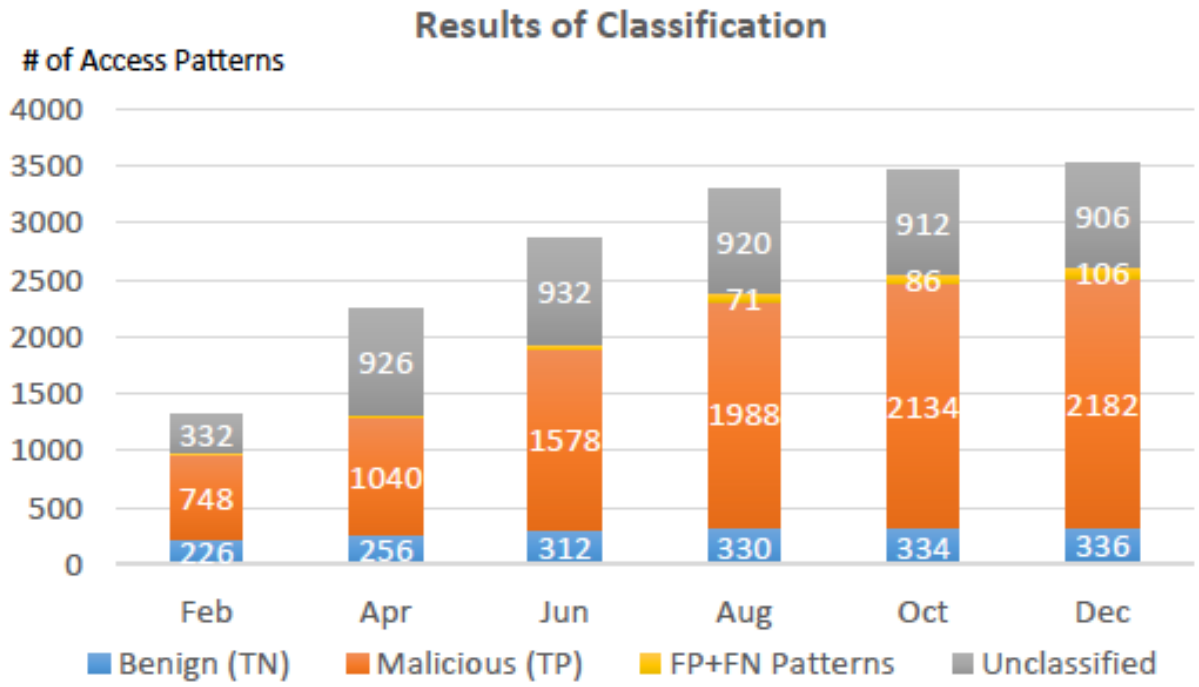
Semi-supervised learning is a type of machine learning that trains on both labeled data (used by supervised learning) and unlabeled data (used by unsupervised learning). It is typically used when labeled data is insufficient and expensive to collect, and a large set of unlabeled data is available. By correlating the features in unlabeled data with labeled data, a semi-supervised learner infers the labels of the unlabeled instances with strong correlation. This labeling increases the size of la- beled data set, which can be used to further re-train and improve the learning accuracy. Semi-supervised learning is popular for information extraction and knowledge base construction. We hypothesize that the process of developing and refining security policies is analogous to semi-supervised learning. Human analysts encode their knowledge about various access patterns into a policy, and refine that knowledge based on examination of audit logs. Because of the difficulty of doing this accurately and in a timely fashion, security policies are generally overly permissive. Semi-supervised learning can automate this process to achieve scalability in policy refinement.

The input to learning is an existing security policy (if there is one), and a set of access events logged from user devices. Each access event entry identifies the subject (i.e., the process or application), the object (i.e., the file or system resource), and the type of execution requested by the subject on that object. Note that audit logs may contain attempted accesses by malicious as well as non-malicious software and users. A main intuition is that non-malicious accesses are much more common than malicious access attempts, and malicious accesses have distinctive features that can be learned by an automated method.

The figure below sketches the approach. The architecture uses three machine learning algorithms that consider different perspectives of the knowledge base and audit logs. The output of these algorithms is fed into a combiner that combines and appends the new knowledge into the knowledge base. This learning process is iterated multiple times until no more new knowledge can be learned from the current audit log input. Finally, the policy generator suggests refinements to the security policy.



This method was tested on the SEAndroid platform, with an input dataset consisting of over 14M denied access events, and an initial security policy containing over 5,000 security rules. The results of evaluation are shown below.




In this graph, blue (true negative, or TN) and orange (true positive, or TP) access patterns are properly classified by our technique. Yellow (false positive (FN) and false positive (FP)) patterns are misclassified, and gray patterns are unclassified. Running time (wall clock time) on this dataset was several hours. In the process, the method classified as malicious more than 200 types of access that are currently allowed by SEAndroid. A number of these accesses have been confirmed as previously unrecognized (and therefore unprevented) attacks on Android devices. Research questions **1**, **3**, and **4** have been answered in the affirmative, while there is still progress to be made on research question **2**.

Mandatory access control has been proposed as an important part of secure systems for several decades. It has not been widely used because of the difficulty of writing security policies for complex systems. We believe the method proposed is a promising first step towards automatically constructing security policies from audit logs collected during normal use of computational devices, and look forward to further exploration of this and related techniques.

### Web-Based Visualization of Snort Alert Data Using Ensemble Approaches (From Christopher Healey)

Prior to and during this reporting period we have continued to extend the prototype visualization system we described at last year's annual meeting. In summary, this tool visualizes correlated netflows and Snort alerts as charts (e.g. bar charts, scatterplots), a simple design rational that was chosen because it is well recognized and well understood by the analysts, and because it has been shown to be

effective for the types of tasks the analysts perform. Based on our model of construction tools designed to fit our analysts' workflow and mental models, each analyst has full control to define the data attributes on the graph's axes, as well as which data to aggregate at different graph positions.

We have further extended our investigation of how ensemble visualization techniques can be applied within our visualization tool. Ensemble visualization studies the problem of visualizing very large datasets made up of "members" that represent events or episodic repetition within the data. In the physical science community, ensembles often encode simulation data, where each member is a simulation run with specific input parameters. In a cyber security environment, an ensemble might be a collection of network data, where each member represents a particular type of suspected attack or collection of network traffic associated with a specific category of class of activity.

We have developed a prototype web-based application, based on our original chart-based netflow visualization tool, to represent netflows and Snort alerts as ensemble members, and to then apply ensemble visualization approaches to present this data. This involved two important challenges: (1) designing a method to represent network security data in a way that fits the "ensemble of members" input requirements for ensemble visualization techniques; and (2) building off existing ensemble visualization methods to visually present netflow and Snort alert data in ways that can efficiently and effectively support network analysts.

For example, we have developed methods to identify patterns in time-varying ensemble members in two different ways. This makes the ensemble approach much more applicable to cyber situation data, since all analysis on network data requires consideration of a time dimension. These techniques have been extended and integrated into our ensemble-based network analysis framework.

Finally, we continue to discuss with ARO IT research staff the possibility of having them act as an intermediary between us and the analysts to validate the practical capabilities of our prototype. The IT research staff are well suited to this role, since they understand the needs of their analysts, and they have the technical expertise to work with us to modify the visualization tool in ways that will best support these needs. We hope to present the enhanced prototype with the ensemble algorithms applied to netflow data to our ARO colleagues to see whether there are promising approaches we can pursue that would be useful for the analysts.

## Scientific Progress Made by Gonzalez Group at CMU

### Instance-Based Learning Theory and Cyber Situation Awareness

The goals of this project

The goal of this project has been to contribute to the understanding of the cyber security analysts' situation awareness in dynamically evolving cyber-attack scenarios. We view the analysts as cognitive beings, with limitations and boundaries in information processing.
We have addressed this goal through two main technical approaches: experimentation with human detection of cyber threats and cognitive computational modeling of human's cognitive processes involved in the detection of these threats. Experiments and cognitive modeling rely on a learning theory

of decisions from experience: Instance-Based Learning Theory (IBLT) (Gonzalez, Lerch, & Lebiere, 2003), which presents decision making as a dynamic process in which analysts interacts with an environment under limited information and uncertainty, and must rely on his/her experience to make decisions. This project contributes to the development of theoretical approaches for understanding, predicting, and supporting the abilities of a cyber security analyst to address cyber attacks. Experimental and cognitive approaches feed each other as new findings from human experiments inform the extensions and developments of IBL models and new IBL models help to make predictions about new experiments. This project also contributes to the practical development of decision support and automated reasoning tools in collaboration with other members of the MURI team.

### Best Accomplishments during 2014-2015

For a reference point of accomplishments this year: the funding available during 2014-2015 was minimal was considerably lower than in the first three years of this project. During 2014-2015, on revisions of manuscripts that were already under review in the past years, making sure that all go through completion. We have also worked on a book chapter which will appear in the book representing the work of this MURI project with the rest of the team. We also made progress in developing a new conceptual model of the cyberwar game, we have defined the formalizations and theoretical rules of the game, and we have developed an IBL modeling platform to be able to execute multi-agent models in the cyberwar context, where all the agents are implemented as IBL models.

## Scientific Progress Made by Cooke Group at ASU

### Mitigating the Information Pooling Bias in Cyber Security Teaming

There is a significant rise in the number of sophisticated and advanced form of threats. To detect advanced forms of threats such as advanced persistent threats and multi-step attacks, effective information sharing and collaboration between the cyber defense analysts becomes imperative. However the innate cognitive biases in cyber defense analysts could hamper the information flow between them that is necessary for detecting such large scale attacks. Teams are known to repeatedly discuss and pool information that is also commonly known to a majority of the team members. They are known to be ineffective in using the unique knowledge available to each team member to make decisions. Therefore, during the past year, we investigated the presence of this team-level bias called the information pooling bias (or hidden profile paradigm in general) in cyber defense analyst teams detecting threat patterns. We designed a prototype collaborative visualization tool that was hypothesized to mitigate any pooling bias. This cognitive engineering-driven tool was compared to off-the-shelf tools.

**Research Question 1**
*Does the information pooling bias affect cyber defense analyst team discussions and decisions?*

The individual analyst or the team of analysts construct new knowledge about emerging attacks out of massive amounts of information, but humans have mental limitations that strain this process and may result in sharing only that knowledge which is common to all team members, thus missing unique information that may better inform decisions. The information pooling bias has been observed in other domains and is hypothesized to occur in cyber security analysis.

**Research Question 2**

*Does a tailor made collaboration tool lead to superior analyst performance compared to using an off-the-shelf collaboration tool such as wiki software?*

Currently, cyber defense analysts are either using off-the-shelf collaboration tools in their work or no collaboration tools at all. Off-the-shelf collaboration tools such as wikis and chat interfaces may facilitate collaboration, but are not developed with the analyst needs and potential biases in mind. We hypothesize that analyst tools that are driven by their cognitive and decision making needs will lead to superior analyst performance compared to other tools.

## Method

A human-in-loop experiment was conducted to investigate research questions 1 and 2. The main thrust of the experiment was in the discussion that took place between the participants. There were two discussion session trials. At the start of each session the participants were assigned individual reports of attack descriptions. Each participant had descriptions about eight attack observations of which four observations were similar in terms of attack type, attack methodology and even the source of the attack was same. Two of the eight attacks were part of a large-scale attack spanning the entire network and the remaining two attacks were just isolated events that had no similarity to other attacks. They were asked to study the alerts and associated descriptions individually for 15 minutes (at the rate of 2 minutes per observation). Then the participants were asked to share and discuss the information available to them to get the big picture of the network situation at hand. They were asked to discuss for 25 minutes (more than a minute to discuss each alert). Depending on the experimental condition they were randomly assigned, participants conducted the discussion either by using the report files provided in the form or slides, or by using off-the-shelf collaboration tools such as wiki software, or by using the proposed collaboration software.

**Procedure.** Thirty teams comprised of three participants each were recruited from the university to work as cyber defense analyst teams in the study. An informed consent form was presented to the participant and they were assigned to the experiment once they provided their consent to participate. The participants were then provided the necessary training for performing the tasks in the experiment.

**Missions.** After the training, the participants performed two trials of discussion on the attack observation reports assigned to them. The report assigned to each of the three participants was different, but contained an equal number of attack observations to read and discuss for experimental control. The participants were alerted to the fact that the reports were not identical and that there could be similarities and connections between their individual reports. The aim of the experiment was to observe and measure whether the participants were incorporating all of the information into their discussion and in making decisions and also whether they identify the multi-step attack by pooling and fusing evidence that is spread across the members of the team.

**Experimental Design.** As shown in Table 1, the experiment proposed is a 3X2 mixed factorial design. Type of tool is one of the independent variables with three levels. For each type of experimental condition, the participants will perform two trials of discussion (a within subjects variable). All participant teams irrespective of the experimental condition will be conducting the discussion without any tool during the first trial. The data from the first trial will serve as the baseline measure of performance and baseline communication data. During Trial 2, the participant teams in the first experimental condition or control condition will again be conducting the discussion without any tool, participant teams in the second experimental condition will be using a wiki style tool during the

discussion and finally participant teams in the third experiment condition will be using the proposed tool during the discussion.

**Table 1** *Experiment Design of the proposed study*

| | Trial 1 - Baseline | Trial 2 |
|---|---|---|
| Tool Type | No Tool - Paper Based | No Tool - Paper Based |
| | No Tool - Paper Based | Wiki tool |
| | No Tool - Paper Based | Proposed tool |

## Measures

**Collaboration**. For the discussion trials, a team performance measure will be measured by taking a ratio of the number of attacks identified by all the members of the team to the total number of attacks. To measure the team's focus of the discussion, the team's communication during the discussion will be recorded. Then the communication will be coded to identify the number of times the participants mentioned each piece of alert information (including alerts unique to them). Then a ratio of the number of times each alert corresponding to an attack was mentioned to the total number of alerts mentioned will be calculated. This will measure the amount the team spent on talking about attacks to talking about the isolated events. Also using communication coded, a ratio of the number of times each alert corresponding to large scale attack was mentioned to the total number of alerts mentioned will be measured. This will measure the amount the team spent on discussing the novel information. Finally post discussion attack inferences will also be recorded as pre-discussion attack inferences.

**Team Process Ratings:** Subjective ratings of different team processes such as acknowledgement, agreement/consensus, argument, reading information, communicating knowledge, inquiring about other's status, clarifying, and updating others on what they are doing were evaluated by the experimenters.

**Workload**. NASA TLX was administered after each trial to assess perceived workload.

## Results

Two main types of measures were collected from the experiment and analyzed. They include measures of performance and discussion focus. The performance measure components include overall attack detection performance, performance in detecting attacks observed by two or more members of the team (termed as shared attacks), and performance in detecting attacks observed by only one of the team members, but which is associated with others attacks observed by other members of team because they are part of large scale attack (termed as unique attacks). The discussion focus measures included the percentage of discussion that involved discussing information shared by two or more members of the team (shared percent) and the percentage of discussion that involved discussing information that is only uniquely available to individual members of the team (unique percent). Analysis revealed that that the distribution of the data is normal and does not violate assumptions of normality.

In Mission 1 all teams in all three conditions used only Microsoft PowerPoint slides during their discussions. However, in Mission 2, based on the experimental condition, teams in different conditions used different tools during their discussion where teams in the slide condition used PowerPoint slides,

teams in Wiki condition used a wiki application and teams in the visualization condition used the visualization.

*Table 2. Descriptives of the discussion focus and overall performance measures in Mission 1*

| | | N | Mean | Median | Standard Deviation |
|---|---|---|---|---|---|
| Shared percent | Slide condition | 10 | 60.5 | 61.2 | 5.03 |
| | Wiki condition | 10 | 64.5 | 65 | 4.2 |
| | Visual condition | 10 | 64.3 | 65.2 | 10.6 |
| Unique percent | Slide condition | 10 | 17.1 | 16.6 | 5.8 |
| | Wiki condition | 10 | 15.2 | 16.7 | 5.4 |
| | Visual condition | 10 | 16.6 | 15.3 | 6.56 |
| Detection performance | Slide condition | 10 | 10.7 | 10.5 | 1.56 |
| | Wiki condition | 10 | 11.9 | 12 | 2.28 |
| | Visual condition | 10 | 11.5 | 12 | 2.27 |

Table 2 presents the descriptive statistics for the discussion focus measures: shared percent and unique percent, and the overall detection performance in Mission 1 by the three conditions. Mission 1 was designed to be the baseline condition for detecting the presence of information pooling bias in cyber defense analyst teams. The descriptives presented in Table 3 show that the mean of all measures in all teams across all three conditions is very similar. These results show that participant teams while performing the cyber-attack detection and forensics analysis focused majorly on discussing shared information (around 60%) compared to the unique information (around 15%). The remainder of their discussion was focused on the noise data.

*Table 3. Descriptives of the discussion focus and overall performance measures in Mission 2*

| | | N | Mean | Median | Standard Deviation |
|---|---|---|---|---|---|
| Shared percent | Slide condition | 10 | 63.14 | 61.39 | 5.4 |
| | Wiki condition | 10 | 67.2 | 66.09 | 8.02 |
| | Visual condition | 10 | 50.29 | 50.17 | 10.46 |
| Unique percent | Slide condition | 10 | 18.51 | 18.41 | 5.2 |
| | Wiki condition | 10 | 17.4 | 18.03 | 6.09 |
| | Visual condition | 10 | 30.14 | 31.92 | 9.2 |
| Detection performance | Slide condition | 10 | 11.4 | 12 | 2.5 |
| | Wiki condition | 10 | 11.8 | 12 | 1.3 |
| | Visual condition | 10 | 14.2 | 15 | 3.1 |

Table 3 presents the descriptive statistics for the discussion focus measures: shared percent and unique percent, and the overall detection performance in Mission 2 by the three conditions. A mixed ANOVA was conducted on discussion focus measures: shared percent and unique percent and the performance measures to see the effect of the different interventions introduced in Mission 2 in comparison to Mission1 where all the teams used PowerPoint slides during their discussion. Therefore the within-subjects factor was the Mission and the between-subjects factor was the condition.

The mixed ANOVA on shared percent revealed that there was a significant interaction effect ($F=10.285$, $p<0.01$). This means that percentage of shared information in the discussion significantly varied between the Missions as a function of the condition. Figure 1 shows the comparison of mean shared percent measure across both Missions and three experimental conditions. As it can be seen in Figure 1, there is drop in shared percentage in Mission 2 in the visualization condition whereas there is an increase in shared information percentage in Mission 2 in the slide and wiki condition.

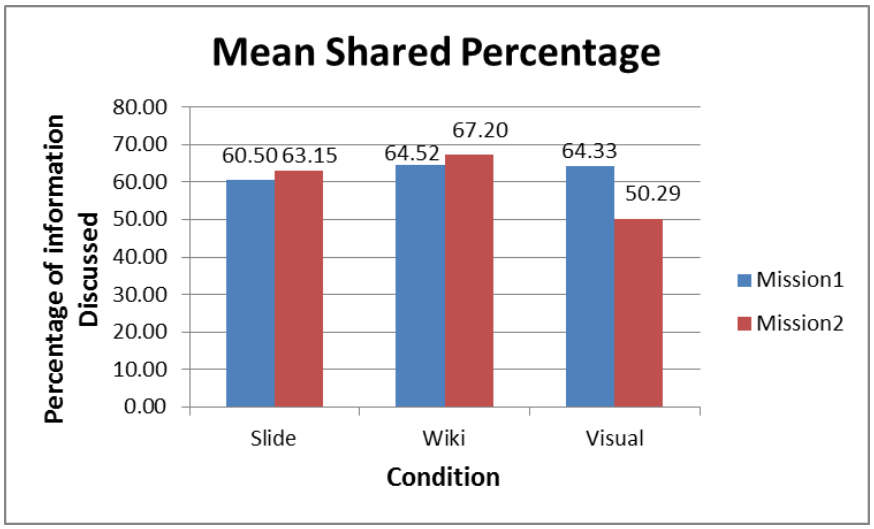



*Figure 1. Bar graphs of shared percentage measure across both Missions and three conditions*

Similarly, the mixed ANOVA on unique percent revealed that there was a significant interaction effect ($F=5.589$, $p<0.009$). This means that percentage of unique information in the discussion significantly varied between the Missions as a function of the condition. Figure 2 shows the comparison of unique percent measure across both Missions and three experimental condition. As it can be seen in Figure 2, there is an increase in focus on unique information in Mission 2 in all three conditions but the increase in visual condition seems greater.

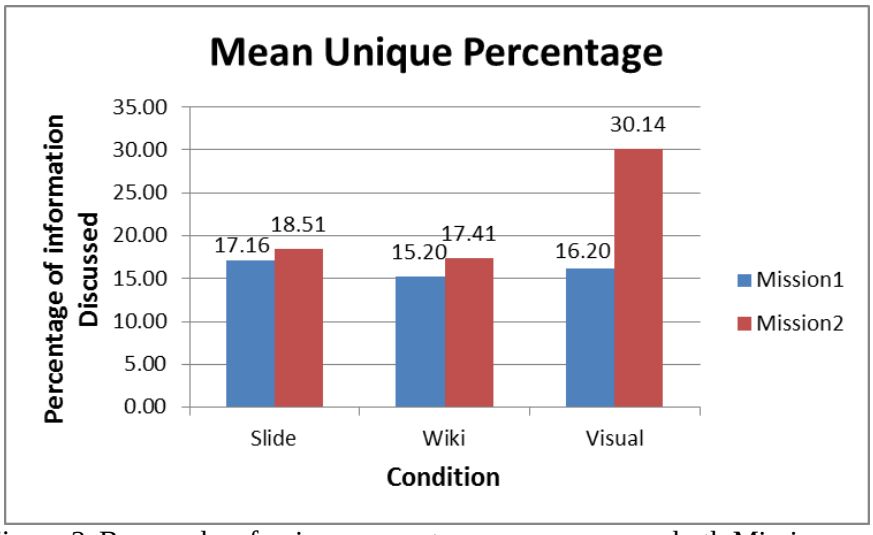



*Figure 2*. Bar graphs of unique percentage measure across both Missions and three conditions

The mixed ANOVA on overall detection performance revealed a non-significant interaction effect (F=3.136, p=0.060). Since the interaction effect on the overall detection performance was non-significant, the overall detection performance was broken down to its constituents: performance from detecting shared attacks and performance from detecting unique attacks. The mixed ANOVA on detection performance of shared attacks revealed that there was a non-significant effect interaction effect (F=0.480, p=0.960) whereas mixed ANOVA on detection performance of unique attacks revealed that there was a significant interaction effect (F=10.082, p=0.001). As shown in Figure 3, there is an increase in number of unique attacks detected in Mission 2 in the visualization condition and the slide condition.

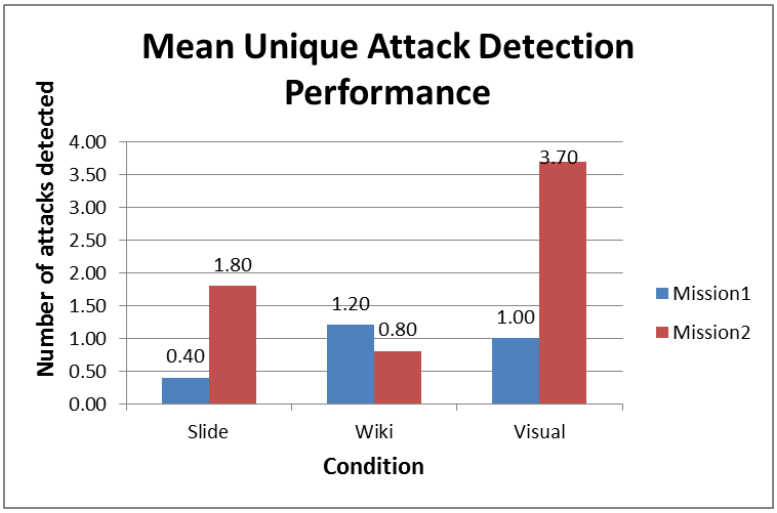



*Figure 3*. Graphs of performance on unique attacks across both Missions and conditions

## Conclusions

This dissertation work investigated the presence of the information pooling bias in cyber defense analyst teams conducting detection tasks as part of forensics analysis and also demonstrated that collaborative visualizations, designed considering human cognitive processes, can be effective in minimizing this bias and improving cyber defense analyst team performance.

Results strongly indicate that all the teams who participated in the experiment exhibited the bias while performing the detection task by spending a majority of time discussing attacks that were also observed by other members of the team, whereas they spent a low percentage of time discussing attacks that were uniquely available to each team member and which were part of a large scale attack.

Specifically, it was observed that when teams did not receive the visualization during their discussion, they discussed shared attack information 63.9% of time which is 3.8 times higher than the 16.9% of time spent discussing unique attack information. However, during Mission 2, when the participant teams in the visualization condition used the prototype collaborative visualization, they discussed shared attack information only 50.3% of time which is only 1.7 times higher than 30.2% of time spent on discussing the unique attack information. This demonstrated a stark increase in the amount of time spent discussing the unique pieces of information when the cognitively friendly visualization was introduced. However bias was observed to still exist in Mission 2.

These findings strongly show that participant teams demonstrated the information pooling bias and this indicates that if forensics analysts collaborate to analyze evidence they may also be affected by the information pooling bias as hypothesized. Detection performance of the teams was also observed to improve in teams who used the tailor-made collaborative visualization tool during their discussions. Teams without visualization on an average detected 11 attacks, whereas teams with the visualization on an average detected 14 attacks. This improvement in detection performance comes from the detection of increased number of unique attacks as opposed to the detection of the shared attacks where the average number of shared attacks detected with or without visualization remained the same, but the average number of unique attacks that was part of a large scale attack detected with visualization was significantly higher than unique attacks detected without visualization.

These findings indicate that the information pooling bias can be minimized (not completely mitigated) in cyber defense analyst teams conducting the detection task as part of forensics analysis by using tailor-made collaboration tools developed taking into consideration the cyber defense analyst's cognitive requirements as hypothesized.

## Scientific Progress Made by Hall and McNeese Group at PSU

### Abstract

This report provides a summary of the activities and accomplishments conducted under the *Computer-Aided Human Centric Cyber Situation Awareness: Models and Experiments in Cognition-Based Cyber Situation Awareness* task led by Michael McNeese and David Hall. This task is part of the multi-year Cyber Situation Awareness Multidisciplinary University Research Initiative (MURI) project funded by the U. S. Army Research Office and led by Dr. Peng Liu. This report covers the period of October, 2014 to July, 2015 (which represents a sixth year extension of the overall project). Details of the overall project and prior year accomplishments can be found in the annual technical reports previously submitted for this project.

During this period of performance this task focused on understanding of the cognitive processes, the context, limitations and issues associated with perception, cognition and decision making for cyber Situation Awareness (SA). Such understanding is a necessary component of addressing the ultimate limited resource for cyber SA: the human cyber analyst. During this period, accomplishments included the following:

- Development of a general architecture and approach for cyber situation awareness incorporating automated reasoning and hypothesis generation with human in the loop context-based reasoning
- Demonstration of the use of Complex Event Processing (CEP) and Coherence Net processing for automated analysis of semantic information related to network situational data
- Acquisition and utilization of Tripwire Benchmark, a system for aggregating cyber-security sensor data from multiple platforms
- Creation of a new set of calibrated test data for use in human in the loop experiments
- Application of the Living Laboratory Framework and the process, developed previously in the study of several human cognitive aspects and how they apply to cyber security

In addition, we disseminated our findings via peer-reviewed journal articles, conference papers, edited book chapters, and presentations. The accomplishments are illustrated in Figure 1.

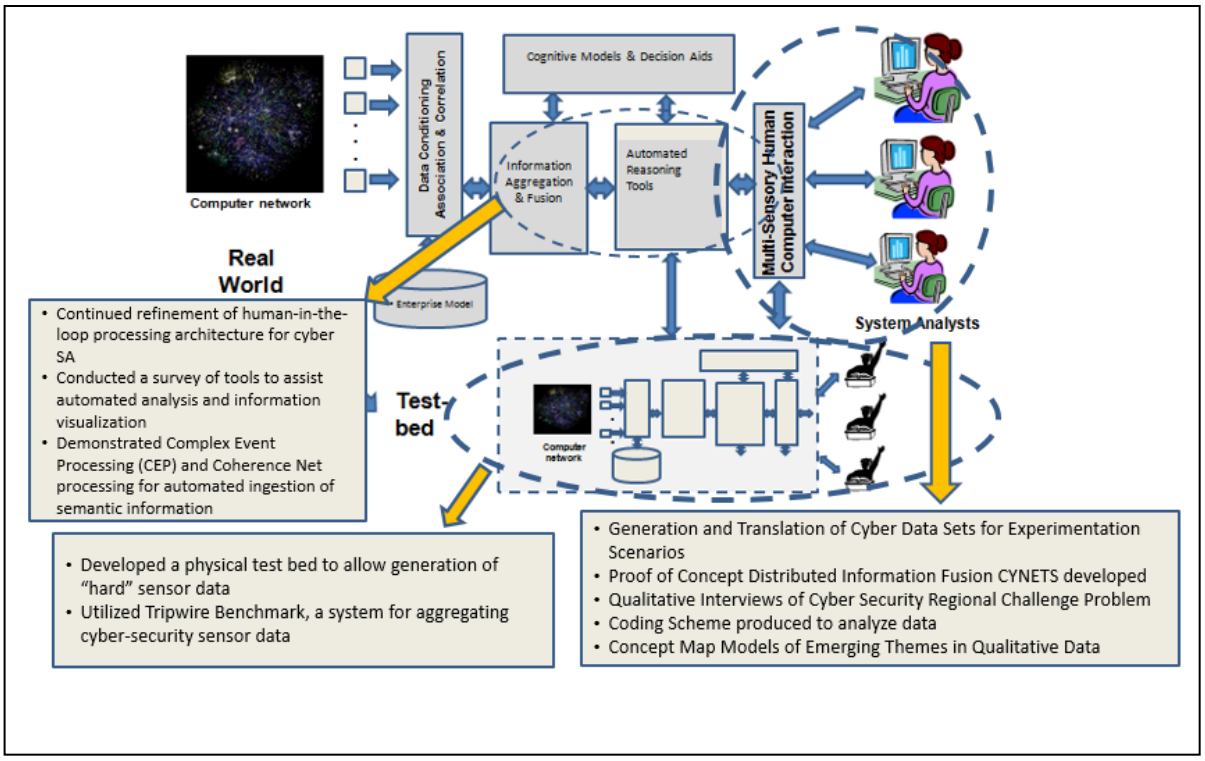



Figure 1: Summary of Sixth Year Accomplishments

## Introduction

The world of cyber security represents a complex environment that may be conceptualized from a number of different world views (mathematical, information and computational science, business intelligence, criminological, ontological, visual analytics, information fusion, big data analytics, cognitive-psychological science, to name a few). As researchers who have historically focused on socio-ecological development of cognitive technologies it is incumbent to ponder what situation awareness or *awareness* represents in the cyber security / cyber defense field of practice. Some believe that answers will be found when there is an increase in the capacity in data accessibility. Others suggest awareness comes through "intelligence" built into computer algorithms or by reducing uncertainty via probabilistic or machine learning computation. Concomitantly, other world views suggest that improvements in awareness come through visualization, visual analytic displays, or through the massive amounts of information that are hidden in "big data". Other perspectives – if even considered – place awareness solely in the mind through consideration of attention and memory processes. More recently, researchers have suggested awareness emerges out of the team mind. While our proposal has touched on each of these perspectives at some point across the last six years of our Army Research Office grant; each one considered in isolation is significantly lacking as it fails to portray the big picture, see McNeese, Pfaff, Connors, Obieta, Terrell, & Friedenberg, 2006, (or what some refer to as the Common Operational Picture of Cyber Situation Awareness in Security).

Indeed, it is no surprise that we conceptualize cyber security as an interdisciplinary system of systems where transformative work is both local and distributed but undertaken by human agents engaged with other agents (human or computational) within an often changing environmental context. From this view, cyber security absolutely is human centered and requires human-in-the-loop processing, contextually driven by change, and must be approached and addressed through problem-based learning. As part of our MURI progress (over the last 6 years) – the notion of awareness and situation awareness that afford cyber defense and successful action requires the timely integration of information, technologies, people, and context if we are to pursue an interdisciplinary system of systems framing of this world. We speak of "worlds" not to be esoteric but to frame the problem not just as improving or inventing cyber security technology but as a challenging world problem that contains multiple layers of complexity that can change and evolve quickly. The world is dis-granular and nonlinear as well as it contains virtual non-physical space (e.g., where hackers attack a software-based system designed to protect computer security), as well as physical cyber security elements, often, which are bridged together through human cognition and action. When considered jointly these elements create what has been referred to as wicked problems (Churchman, 1967).

In reality - there are multiple kinds of awareness present in the system, emergent across time and space, represented in various ways to human and agent; distributed throughout the cognitive system. This is our collective view of what awareness means within cyber worlds. Hence, we refer to this niche as Cyber Distributed Cognition. Based on our own work the following elements are considered primary research missions within this niche:

I. Opportunistic Problem Solving in Cyber Operations
II. MetaCognitive Reflections about the Threat
III. Learning and Spontaneous Access of Knowledge in Context

These missions are both interactive and iterative with each other holistically. Because we believe that cyber situation awareness is an immersive, evolving state that draws from cognition into the context as opposed to just some static knowledge state in the head, our missions point to different ways of thinking about awareness as it plays out within cyber distributed cognition. The missions also formulate some of the backbone of discovery that underlie our actual research objectives over the past year.

*Framing the Problem Space – Use of the Living Laboratory (LLF).* As mentioned one's worldview can intimately determine what is a problem and what is not a problem dependent on where a researcher is "coming from". Because we view cyber SA as distributed, cognitive work that is mutually influenced and effected by the context of action (this is a cognitive engineering world view, see McNeese & Vidulich, 2002) it is incumbent to utilize our own Living Laboratory Framework –LLF- (McNeese, 1996) to discover and explore problems within cyber security/cyber defense. Figure 2 shows the Living Lab Framework. As one can see the central heart of the framework is that of discovering - defining – exploring problems to learn new ways of solving problems. Clearly this framework then enables a *problem-based learning* (Bransford, Brown, & Cocking, 2000) approach to human centered cyber SA. Problems come into focus through a variety of means. This is captured in the framework by the interactions of the four elements: ethnography, knowledge elicitation, scaled world simulations, and reconfigurable prototypes. Problems can be informed from the top-down -through theoretical positions- and from the bottom-up - through practice. Practice in the real world as we know is coupled to extant problems that occur as users experience them in differing ways. This excites the bottom-up processes in the LLF that focus on what gets done in cyber security (in particular, cyber situation awareness) and how people utilize technology

to accomplish work. As related earlier much of this work is distributed and complex. Concomitantly, problems are also coupled with theory or theoretical positions taken by researchers.

Theory provides a view of what could happen in cyber security by postulating hypotheses about how human-cognitive agents transform their world. Because our world-view necessarily incorporates human-in-the-loop processing of cyber security, practice is typically known (heeded) by the experience that an agent (analyst, operator, or user) encounters while involved with distributed work. At the core of the LLH then is the coupling of *theory-problems-practice* and the ways they are informed by feedback from the four elements that can provide additional enhancements of data/information/knowledge. As learning ensues in a given element it feeds-forward to setup processes in other elements as well, and also improves comprehension. Research coupling among these elements also may yield secondary increases regarding *use* and *modeling.* By cycling though these elements the framework it affords a living ecosystem approach to distributed, cognitive work that promotes an interdisciplinary, transformative, systems-level thinking in advancing success in cyber security worlds. We will return to unpack this figure with more specificity as we get into the specific activities of year six of the MURI research a bit further on in the report.

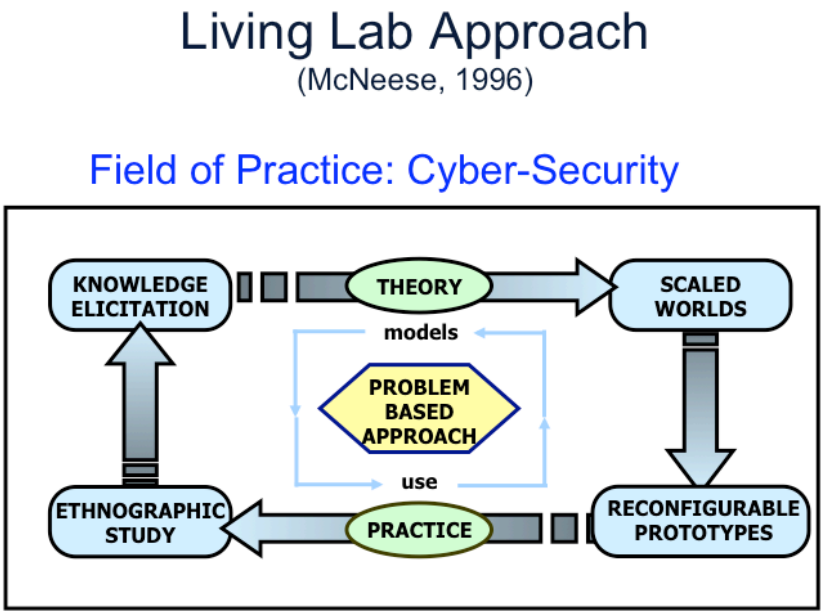



Figure 2. The Living Laboratory Framework

*Engaging the Problem Space – Distributed, Cognitive Work.* We begin by reviewing some of the attributes we know about the problem space. Our framing of the problem is best taken as 'situating cyber situation awareness' paper (McNeese, Cooke, & Champion, 2011) developed directly from our MURI work. That paper enabled a distinctive cognitive engineering perspective to understanding cyber security worlds, which has continued in our research throughout the grant. So the first premise is that awareness within cyber worlds is work that engages cognition within specified contexts wherein technology developments improve aspects of sense-making, decision making, problem solving, and/or action potentials. This coincides with a human centered approach where cyber security is viewed as first and foremost as distributed, cognitive work wherein tools and technologies support cognitive work to improve performance (eliminating problems, enhancing capabilities, removing constraints, adapting response). Taking that as our baseline, lets delve in more depth as to what this means. The attributes

we find embedded with the cyber security world embroil around difficulties humans have as agents engaged with a complex context. Figure 3 summarizes these problem attributes on a general level and the consequences that emerge for humans.

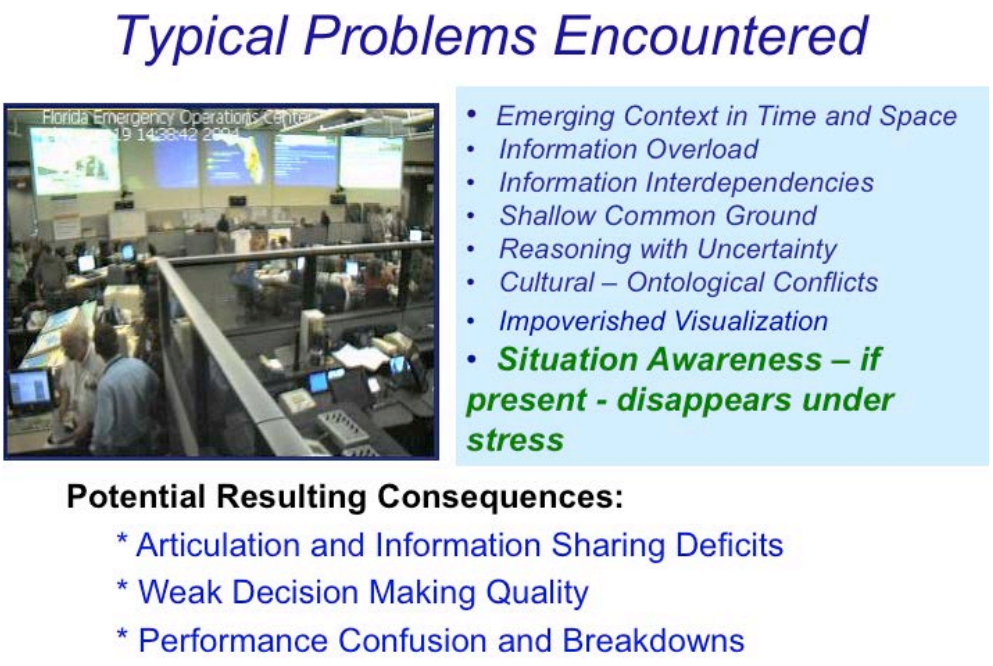



Figure 3. Problems Encountered in Distributed Work Settings

**Research Accomplishments**

Considering the above problems and issues that are pertinent within cyber security operations, there are three specific areas (premises) we wish to look at:

1) Cyber-situation awareness as distributed cognitive work as performed in given context, field of practice,
2) Cognitive work will focus on human-systems integration centered on information fusion for both hard and soft sensor data,
3) Cyber operations potential can improve with apropos teamwork (both within and across team performance).

Because our overall worldview is to improve cyber SA via a human centered design process using the Living Lab Framework it necessarily adheres to understand distributed cognition wherein information, time, place, people, and technology are all distributed in unique orchestration. As such cyber distributed cognition is the bedrock from which we have evolved our overall approach to research, design, and experimentation.

The overall goal is to approach 'knowledge as design' and leverage what has been learned in prior years in knowledge elicitation, previous simulations, and use of cognitive technologies to support enhance work. As we approached the 6th and final year there were two specific objectives to accomplish to fulfill further understanding about how humans can increase productive activities and adaptive work in cyber

operations. Objective 1 focused on the design / test of a new *proof of concept* human-in-the-loop simulator which we call **CYNETS.** This stands for Cybernet Team Simulation. This work represents more of our need for a quantitative test bench to generate experimental studies that look at how cyber SA forms both within individual and team orchestrations. Objective 2 focused the use of a Cyber Threat regional exercise which our SRA students participated in as teams. This objective represents more of a need for qualitative data directly taken in the form of knowledge elicitation interviews, which can then be used to propagate initial concept map-based models. In both objectives, the intent is to create understanding in this realm or to design new tools that can further elicit critical behaviors that are salient within cyber distributed cognition that are useful for the design of innovative tools, interfaces, models, or cognitive aids of the future.

Objective 1, 2, and 3 utilize the Living Lab cycle fully as the current work first focuses on building a scaled world simulator and design infrastructure prototype based on prior knowledge (inclusive of previous knowledge elicitation with some experts at our early workshop that Nancy Cooke organized in Phoenix), as well as learning different aspects of the cognitive-contextual basis of distributed work from the previous simulations we built during the MURI (CyberCITIES, TeamNets, and IDSNets) and cognitive technology prototypes use (Visual Analytics Test-bench, Giacobe, 2013). Additionally, the Living Lab is utilized currently to discover new dynamics relative to student teams engaged in a threat exercise wherein problem finding-solving, decision making, and planning are all evident for successful performance. We also worked with some early modeling concepts predicated on the output of the interview coding that was performed with student interviews.

**Part 1: CYNETS Simulator Proof of Concept**

*Preparations and Development.* Inherent in our simulation – CYNETS - was the desire to create scenarios that built off of realistic hard data to provide a solid scaled world feel wherein the collective demands on distributed teams would be bound to both hard and soft data integration. Also, we desired a simulator with a scenario that required discovery-information seeking, team communication/coordination, cognitive processing, and therein a task that was ill/defined and uncertain to a degree that would enable the necessity of developing cyber SA.

CYNETS task. The work they performed was typical cyber-defense activities. They were given remote access to two Linux and two Windows-based servers to defend from live "red-team" attackers. They were also provided dynamic injects of tasks they were asked to perform – typical systems administration tasks, account creation, database updates, etc. They had full administrative access to the systems they were defending, so they could do anything they wanted. Typical tasks included enumerating and securing accounts with administrative access (changing from default passwords), identifying and updating software with patches, modifying configuration of software to turn off unneeded services, etc. During the exercise, the students needed to identify what was wrong (configuration, patches accounts, services), figure out if attackers were utilizing those vulnerabilities to compromise systems, and turn off attacker access if they were able to locate that the attacker had gained access.

Simulation Data. To develop hard data fusion elements the experimental simulation data was created in the lab environment from a similar perspective. The simulated data was fabricated from a network of computers in the laboratory that simulates an active network of computers from a fictitious organization called "ABC" (see Figure 4). The ABC network includes three servers and 25

workstations. The data that was provided to simulation exercise analysts included a 24-hour period of logon/logoff log data from a Windows 2012 server for the entire network.

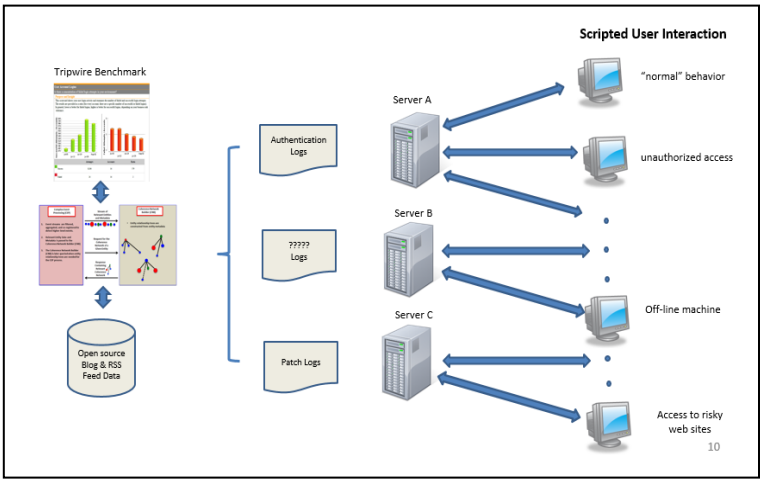



Figure 4: ABC Simulated Network

In this 24-hour period, accounts were logged on and off of computer systems to create actual log entries in the Windows Security Log of the server. While the actual events of successful logon and logoff events are entered into the Security Log of the authentication server, these are not the only events that are generally displayed there. A windows domain treats computers in a similar way to the way it treats users. They must also log on and off. However, a systems authentication is more automated. Also, as a user authenticates and accesses networked services, other authentication records are also in the log to include every time a networked user accesses a different network device. This noise of normal activity often clouds the real issues of authentication failure and account misuse. The data set that was presented to simulation participants had some level of normal noise, but generally was limited to successful logon, successful logoff and unsuccessful logon events. Embedded in the presented authentication data was a series of failed logon attempts, followed by an eventually successful event. This simulated a password-guessing activity that resulted in a compromised account.

Additionally, the same 24-hour period was used and a number of viruses were copied on to the computers. The antivirus program was allowed to detect these files and take appropriate action – either delete or quarantine the files with the malicious code. Together with the updates of new antivirus definitions, these two types of records were presented in the antivirus data. To simulate unsuccessful antivirus actions, anti-virus alerts were fabricated repetitively on one system. This mimics the behavior of some antivirus applications – where a suite of malware is installed on a system that re-installs other parts of the suite if they are removed. The undetected malware is indicated because of the repeating successful removal of several sets of other parts of the suite. Together with an outdated set of virus definitions, an analyst is led to the conclusion that the system must be infected with malware that is not detected by the old set of definitions.

The final set of data is patch management. In this case, we created a set of records of normally applied updates. However, we also intentionally left one system offline for a period to show the lack of updates being applied to that system. Additionally, we filled the hard drive of another system to prevent it from having patches applied. This system showed "failed updates", primarily because the drive was full. A

network analyst seeing records from these systems would be able to interpret that the systems needed hands-on attention to figure out why they are not receiving their patches.

*Methods.* Three triad teams were recruited from an Information Sciences and Technology (IST) course within the College of Information Sciences and Technology (IST) at the Pennsylvania State University. Each individual was randomly assigned to one role for the simulation either (1) Windows Authentication Analyst (WAA), (2) Anti-Virus Analyst (AVA), or (3) Windows Update Analyst (WUA). Each role is responsible for reactionary machine and problem identification through the simulated logs as previously described.

Upon entering the lab and signing the informed consent forms, participants receive their randomly selected role and are given a pre-trial demographics survey. Subsequently, they are directed to read through a role-specific PowerPoint presentation for training. After all participants have completed the training presentation, a 5-minute training scenario is started to allow the participants to get familiar with the interface and the task. When the training scenario is finished, the participants are given a survey to quantify their individual situation awareness (SA) using NASA-TLX (Hart & Staveland, 1988), SART (Taylor, 1990) and MARS (Matthew & Beal, 2002).

After the survey is completed, participants are given an additional training scenario followed by another individual SA survey. Following both training scenarios, the participants are given a quick debrief about the scenario and the proper response. Next, the first performance scenario is started and once complete is followed by the same individual SA measures but with the added Shared SA Inventory (SSAI) (Schielzo, Strater, Tinsley, Ungvarthy, & Endsley, 2009). Subsequently, participants are asked to complete the second performance scenario and the same individual SA and SSAI surveys. Upon completion of the final survey, participants are debriefed about the fictitious nature of the scenarios and thanked for their service.

*Results.* The simulation was tested initially with 3 teams to assess feasibility and capture the performance measures mentioned above. Everything worked well in the simulation, and students were able to perform in the role of individual and team cyber analyst duties in determining routine and threat activities as part of their task. While the initial proof of concept was conceptualized, implemented, and tested- and met the expectations of the experimenters, more robust testing and experimentation is desirable. This is discussed further in the future work section below.

*Implications.* The CYNETS scaled world simulation represents the development of a challenging cyber operations environment that emulates real world threat assessment that involves distributed cognition across individual and teamwork functions. As such it provides a capability for extending understanding of hard (and potentially soft data fusion) within an emerging milieu. The implications are that the study of the problems mentioned at the beginning of this report can be brought into the lab setting and studied for further illumination of situation awareness within cyber defense. Further work on cognitive technologies that are human-centered in design can be embedded within the information architecture underlying the simulator designed to undergo precise human-in-the-loop testing to determine how they improve human/team performance.

**Part 2: Cyber Threat Regional Competition (Qualitative Study)**

*Preparations and Development.* We were given an opportunity to have access to an IST Security Club project wherein members competed in the *Mid Atlantic Collegiate Cyber Defense Competition*. This

allowed us as researchers to develop a qualitative study to determine how they would problem solve and make decisions when presented with an engaging Cyber Security Threat Situation. As part of the competition they were asked to participate in a challenge problem.

*Challenge Problem*. The following paragraph describes what they did on the challenge problem in the regional competition:

> The work they performed was typical cyber-defense activities. They were given remote access to two Linux and two Windows-based servers to defend from live "red-team" attackers. They were also provided dynamic injects of tasks they were asked to perform – typical systems administration tasks, account creation, database updates, etc. They had full administrative access to the systems they were defending, so they could do anything they wanted. Typical tasks included enumerating and securing accounts with administrative access (changing from default passwords), identifying and updating software with patches, modifying configuration of software to turn off unneeded services, etc. During the exercise, the students needed to identify what was wrong (configuration, patches accounts, services), figure out if attackers were utilizing those vulnerabilities to compromise systems, and turn off attacker access if they were able to locate that the attacker had gained access.

*Methods.* The participants for the qualitative study were recruited from the team of students that were participating in the National Collegiate Cyber Defense Competition (CCDC). After the project was described to students. Informed consent forms were signed, and the participants were questioned about their team experiences, training and preparation activities, and understanding of the competition and their teammates. The interviews were recorded and notes were also taken to supplement the digital recordings.

When all of the interviews were completed, the digital recordings were sent to a transcription service that transcribed the data word-for-word. In instances where the recording was inaudible the handwritten interviewer notes were used for clarification. All of this data was analyzed by two of the researchers collaboratively. Key phrases were pulled from the transcript and put into a spreadsheet. Once the key phrases were identified, the same researchers worked together to identify themes and categories in order to create the coding scheme (see Figure 3). This coding scheme was again collaboratively used to classify each of the key phrases previously identified. In cases in which a classification did not exist, the coding scheme was modified and the process continued as normal.

*Results.* The outcome of the coding scheme application resulted in specific frequency of occurrence of codes across all interviews. This highlights the nature of distributed cognition, situation awareness, and individual and team cognition as it relates to students identifying, exploring, and solving the challenge problem(s).

In addition to understanding the content of the entire set of interviews vis-à-vis the coding scheme, a plan was derived to produce a descriptive model of the student's distributed cognition to ascertain how situation awareness emerged within knowledge, context, and process. The use of concept mapping (Zaff & McNeese, 1993) was chosen as a flexible, lightweight kind of cognitive model and was collaboratively formulated by the same researchers who coded the interviews - by utilizing the raw text of the interviews and the frequency occurrence produced by the results of the coding scheme. An overall plan was generated to produce an integrative, overlay model of cognition (see Figure 5).

| | | |
|---|---|---|
| 4 | **Problem Solving** | Activities necessary for identifying, addressing, and resolving issues |
| 4.1. | *Strategies plan of action* | |
| 4.1.1. | Shared across the team | |
| 4.1.2. | Individual strategies | |
| 4.2. | *Processes* | Articulated written or unwritten plans necessary to address problems |
| 4.2.1. | *Actual* | What were some of the processes of problem solving |
| 4.2.2. | *Adaptive* | Flexibility of processes when new information was presented or something was found to not work |
| 4.3. | *Problem Monitoring* | Activities and techniques for tracking and documenting problems |
| 4.3.1. | Initial identifications of problem | |
| 4.3.2. | Updating problem | |
| 4.4. | *Process Monitoring* | Tracking and documenting of the processes for problem solving |
| 4.4.1. | *Strategies* | is there monitoring of those actions used to problem solve |
| 4.4.2. | *Outcomes* | are the results desired or appropriate to the task |
| 4.5. | *Reassessment* | |
| 4.6. | *Errors* | What happened when there were errors? |
| 4.7. | *Tools* | |
| 4.7.1. | Information Technologies | |
| 4.8 | Priorities | |
| 4.8.1 | Updates to | |
| | | |
| 5 | **Planning** | Activities for the purpose of having the necessary skills, personnel, and knowledge to be successful |
| 5.1 | *Team based planning* | Activities coordinated among the team for planning purposes |

Figure 5: Coding Scheme used to Analyze Interviews

To initiate this plan the first phase accomplished included creating a declarative concept map to represent some of the major findings in the coding scheme (as applicable to the actual interview text phrases) to come up with a first-level model of knowledge underlying distributed cognition in cyber operations teamwork. The declarative concept map in turn represents element # 1 in the overall overlay: *intention.* The other elements (*solution path*, *teamwork in evidence*, *cognitive processes demonstrated*) would also need to be developed to completely in the next phase of future work to completely propagate the entire overlay cognitive model. The first phase model (see Figure 6) is heavily informed by the activity of planning and re-planning, and determining what role uncertainty plays in accomplishing the overall challenge problem. As we perused this initial concept map there was much to be learned in how individuals and teams formulate what the challenge problem consists of, and in turn how to begin tackling it. All of this is valuable for understanding comprehension of cyber threat activity, and how this might be improved with new cognitive technologies that would enable information fusion and potential gains through collaborative teamwork.

*Implications.* It is evident that students working together in teams often struggle to understand how they will solve the problem given to them and how they can work together to reap the benefit of their collective talents. In newly formed teams this is difficult process as it minces strategic knowledge resident in teamwork processes with specific knowledge needed to solve the problem at hand.

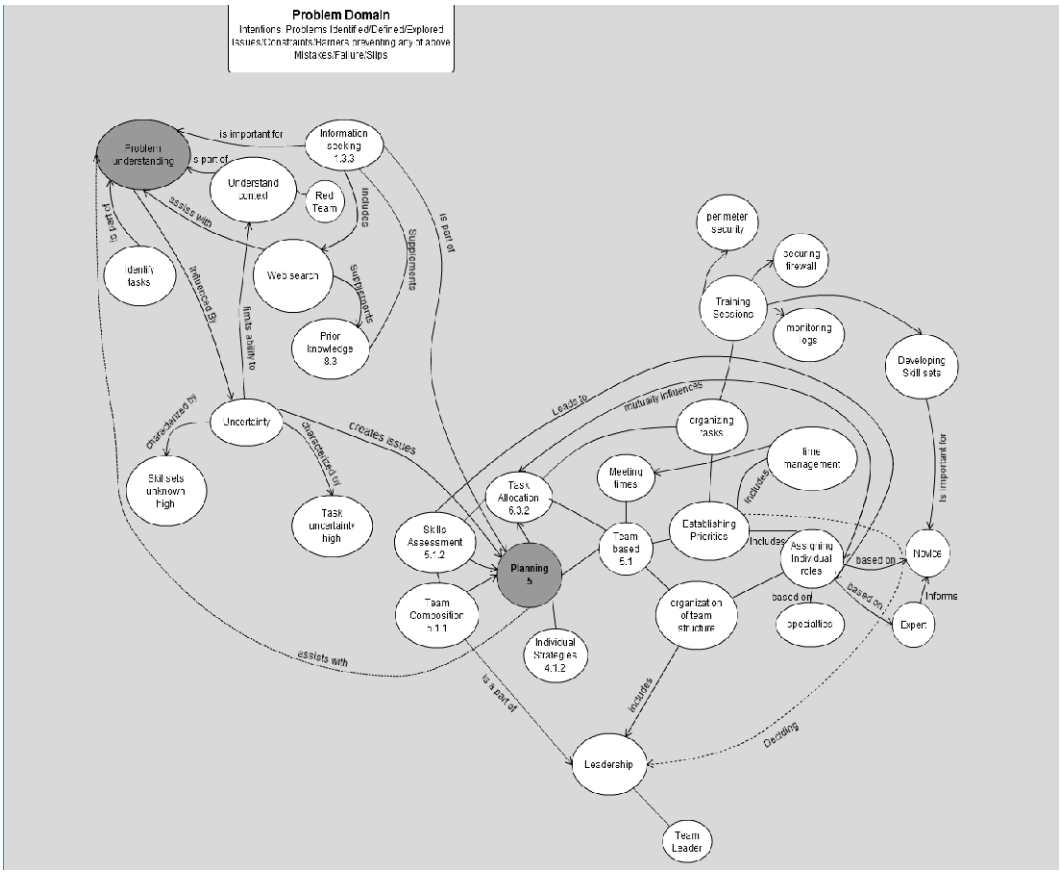



Figure 6. Declarative Concept Map of Intentions-Solution Paths

Furthermore, the management of their intentions becomes a reified issue in that they have to spend time figuring how to work as individuals but yet as an interactive team , including defining "function allocation" (i.e. Who will do what when with what tools?). Although this was a first-level concept map specifically focused more on planning – it is the first of several concept maps that could be generated as part of the layered representation.

## Discussion/Future Work

The work undertaken represents further effort to open discovery, understanding, and prediction as to how situation awareness emerges in distributed cyber operations (both individually and in teamwork). While this is a lofty goal, the research described above (coupled with our five previous years of MURI research) has begun to make necessary in-roads in these areas. In particular, we have designed, implemented and provided an initial proof of concept for the CYNETS scaled world simulation involving distributed information fusion surrounding an emergent adversarial threat situation. While the first experimental design and test of the simulation only involved the incorporation of hard data fusion, the scaled world is designed to include soft data fusion in future studies to further extrapolate nuances of cyber situation awareness as cyber operations are employed in both routine and non-routine opportunistic problem solving sets.

Our use and testing of the scaled world using scenarios involving human-in-the-loop testing with Security and Risk Assessment (SRA) students within the College of Information Sciences and Technology

validates that it is possible to create a realistic emulation of cyber security using typical data expressions and use from day-to-day cyber analyst activities. The simulation affords analysis of individual cognitive processing as well as team cognitive processes to comprehend and discover specific problems and issues that arrive in predicting correct answers or solvation of complex problems. Having the availability of this type of simulation gives an additional tool to breakdown the reasons for individuals and teams not coming up with the absolute correct answers. This purports a "failure-driven learning" approach wherein over time correct answers may be discovered through use and interaction.

Concomitantly, it gives an ability to assess and analyze why wrong answers or procedures occurred potentially giving rise to detect and isolate bugs in cognitive models, and/or barriers to learning how cyber situation awareness comes into existence. Learning why SA does not envelop in the individual and in turn the group provides the basis upon which human-centered cognitive technologies can be developed (as opposed to just blindly throwing technology to the wall to see what sticks).

In addition to developing and testing the CYNETS simulation we were provided an additional unique opportunity to have access to IST students participating in a regional cyber security exercise. This access allowed us to interview students especially as to how they plan to attack a cyber threat situation (again both individually and in teams) and allowed a different kind of exploration as to how students identified, defined, investigated, and solved problems (or not) but from an alternative mode of understanding in contrast to an experimental design and simulation-based study. It is important because; (1) it was deemed state of the art for student teams (circa 2015), (2) it was provided by governmental officials who are fully aware of the embedded issues and constraints and therein represented what would be indicative of wicked problems in the literature (Churchman, 1967), and (3) these students will very soon be practicing cyber analysts so it is important to see how they interpret the cyber word and see what their shortcomings are in terms of distributed cognition and cyber situation awareness as they represent the new generation who will be combating threats of the future.

Many of the contextual and human-centric elements of decision making came into play (e.g., how they setup teams and utilize expertise, how they planned and re-planned the problem (metacognitive actions), how they knew how far to go in terms of pursuing a given path of solution, how they make team decisions, etc.) really influence their overall awareness of who they are, how things work together, and how the emerging context restrains what they can do in a limited timeframe (time pressure). Like many complex problems uncertainty and reasoning about uncertainty will impact the directionality of interdependent problem elements and how they become aware of what a threat is – where it exists at – and whether it is current.

Our intent with the qualitative interviews of students was to apply a coding scheme relative to the interests we have outlaid in work for the last six years (i.e., mainly pursuing a distributed cognition worldview that emphases learning and the evolving transactions between agents (human or computational) and the environment). Once our encoding scheme was applied to interviews we were able to use it to engage development of an initial concept-map based descriptive model (basically focused on planning and how people tackle the problems resident in the exercise). Concept maps afford descriptive based cognitive models which can be flexibly used in different ways but mainly as lightweight knowledge representation typologies emanating from knowledge elicitation activity (Zaff & McNeese, 1993). We will discuss more about this below in the future work section.

Our overall goal with the modeling part of the Living Lab Approach, however, is to generate what we refer to as a layered, declarative concept map. This models declarative (and to some extend strategic)

knowledge resident in a novice or expert cyber analyst for a given challenge problem within a specified context. As such it employs both cognitivistic and contextualistic layers of understanding and thinking as a person or team evolves through solvation of the problem presented. Because the map is heterarchical and is entrenched within the concept-relation-concept syntax it is maximally flexible and not over constrained. The coding scheme and concept maps of interviews of novice-level students can be useful to contrast and compare against expert concept maps for further elucidation, and inspire specific requirements for training.

In summary, much has been discovered. However, still more needs to be discovered about distributed cognition, information fusion, and teamwork as it contributes to establishing situation awareness in cyber defense. The approach taken here has always been to keep cycling to various components of the Living Lab as opportunity presents itself with eventually the intent to intervene in real world practice with; a) effective cognitive technologies that truly impact positive *use* or b) Innovative training for individuals and teams involved in complex cyber security problems. We turn now to discuss potential future work that directly follows directly from our research activities from this last year.

*Future work.* If one steps back from what has been accomplished this last year, it clearly sets up some new research channels and extensions that could come into effect. We will briefly discuss what needs to be done in the next phase to further establish this line of research.

First, for the experimental research we feel that the next step is a full-scale experimental study involving CYNETS. Our hope would be to run an experimental design wherein hard fusion is crossed with soft fusion access. In this case soft fusion represents specific intelligence gathered on the threat that emerges during the course of the scenario. This would complement the hard fusion component and provide an additional dynamic in the teamwork component. This would provide a fuller scale test and actual experimental evaluation for publishing (assuming significant effects were obtained). The orchestration of the soft fusion element could be information provided only to one team member at a given point in time (simple soft data fusion) or unique information could be given to all three team members at different points in time (complex soft data fusion). There is experimental evidence that suggests team members only share that which is unique, which if true really limits the collective induction possibilities in the cyber context. Our intent would be to try to utilize ROTC students (as a kind of more DoD-aware student base) and compare with IST/SRA students (who are probably more aware of the technology and security-risk aspects of cyber systems).

Second, the coding schema data can be further propagated as a more integral concept map that involves layered representation to couple together different perspectives on knowledge that underlies situation awareness and distributed cognitive process. The first step would be to produce additional declarative, procedural, and strategic knowledge-based concept maps according to the planned overlay concept mapping typology (see Figure 6). In the tradition of the AKADAM techniques (see Zaff, McNeese, & Snyder, 1993) it is the intent to use the lightweight concept map model as the basis for; (1) establishing user needs and (2) defining new interface or cognitive technologies to obtain what Perkins (1989) refers to as 'knowledge as design'. The trajectory would be to use the entirely propagated layered concept map across every element as a basis for prototyping new designs that improve situation awareness in individual and distributed cognitive activities.

Third, the results from the experiment can be merged with the qualitative study to mutually inform each facet of our research (e.g., the research independent variables can be directly derived from qualitative

data, and likewise the results of experiments can inform better cognitive models of individual cyber analysts and teams of analysts as they engage situation awareness in this kind of context.

Finally, another future goal would be to expound on descriptive lightweight models and create new middleweight models in the form of abstraction hierarchies and the cognitive decision ladder (Rasmussen, Pejtersen, & Goodstein, 1994). These models emphasize both structure and function more than concept maps but are given to make extant the actual contextual variants as well as providing representation of insights when learning proceeds. This is important because both kinds of models set up the cognitive systems engineering of adaptive resiliency systems of awareness in cyber operations which is need where evolutionary uncertain information fusion foments across a highly distributed environment. Eventually, the goal would be to learn from the discoveries inherent in student exercises as well as the experimental designs in a way that really strengthens and reinforces the cognitive models and ensuing technologies that are waiting to be developed for the next generation.

**References**


- McNeese, M. D., Mancuso, V. F., McNeese, N. J., & Glantz, E. (2015), "What went wrong? What can go right? A prospectus on human factors practice", to appear in *Proceedings of the 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences*, AHFE, July, 2015, Las Vegas, NV
- Hall, D., McMullen, S. and C.M. Hall (2015), "New perspectives on Level-5 information fusion: The impact of advances in information technology and user behavior," accepted for the IEEE 2015 *International Conference on Multisensor Fusion and Integration for Intelligent Systems*, Sept. 14 – 16, 2015, San Diego, CA.
- Hall, D. L., J. Graham and E. Catherman, (2015), "A survey of tools for the next generation analyst", *Proceedings of the DSS Sensing Technology and Applications Analyst: Next-Generation Analyst III,* 20-24 April, 2015, Baltimore, MD
- McNeese, M. D., and D. L. Hall, editors, *The Living Laboratory: An Integrated Problem-Centric Approach to Cognitive Systems and Teamwork,* (in preparation)
- D., and D. L. Hall, D., G. Cai and J. Graham (2015, in press), "Empowering the next generation analyst" chapter in *Information Fusion in Crisis Management*, ed. By G. Ragova and P. Scott, Springer.
- N. Giacobe and D. Hall (2015), Research Opportunities and Challenges for Cyber Systems Risk Management, June 30, 2015 (27 pages), technical report for Penn State Applied Research Laboratory
- Bransford, J. D., Brown, A. L., & Cocking, R. R. (Eds.), (2000), *How People Learn: Brain, Mind, Experience, and School,* Washington, DC: National Academy Press
- Churchman, C. W. (1967), "Wicked problems", *Management Science*, *14*(4), 141–142.
- Hart, S., & Staveland, L. (1988), "Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research", in P. Hancock & N. Meshkati (Eds.), *Human Mental Workload* (Vol. 52, pp. 139–183): North-Holland.
- Giacobe, N. A. (2013), "A picture is worth a thousand alerts", *Proceedings of the 57th Annual Meeting of the Human Factors and Ergonomics Society* (pp. 172-176), San Francisco, CA.
- Matthew, M. D., & Beal, S. A. (2002), "Assessing situation awareness in field training exercises", *US Army Research Institute for the Behavioral and Social Sciences*.
- McNeese, M. D. (1996), "An ecological perspective applied to multi-operator systems", in O. Brown & H. L. Hendrick, (Eds.), *Human Factors in Organizational Design and Management* - VI. (pp. 365-370), The Netherlands: Elsevier
- McNeese, M. D., Cooke, N. J., & Champion, M. (2011), "Situating cyber-situational awareness", *Proceedings of the 10th International Conference on Naturalistic Decision Making* (NDM 2011), 31May-3 June, Orlando FL.
- McNeese, M. D., Pfaff, M., Connors, E. S., Obieta, J., Terrell, I., & Friedenberg, M. (2006), "Multiple vantage points of the common operational picture: Supporting complex teamwork", *Proceedings of the 50th Annual Meeting of the Human Factors and Ergonomics Society* (pp. 26-30), San Francisco CA

- McNeese, M. D. & Vidulich, M. (Eds.). (2002). *Cognitive Systems Engineering in Military Aviation Environments: Avoiding Cogminutia Fragmentosa*. Wright-Patterson Air Force Base, OH: Human Systems Information Analysis Center (HSIAC) Press.
- Perkins, D. N. (1986), *Knowledge as Design,* Hillsdale, N.J.: Lawrence Erlbaum Associates
- Rasmussen, J., Pejtersen, A. M., & Goodstein, L. P. (1994), *Cognitive Systems Engineering,* New York: Wiley
- Scielzo, S., Strater, L. D., Tinsley, M. L., Ungvarsky, D. M., & Endsley, M. R. (2009). "Developing a subjective shared situation awareness inventory for teams", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol 53: 289)
- Taylor, R. M. (1990), "Situational awareness rating technique (SART): The development of a tool for aircrew systems design", *Situational awareness in aerospace operations,* AGARD-CP- 478. Neuilly Sur Seine, France: NATO-AGARD, 3/1-3/17
- Zaff, B. S., McNeese, M. D., & Snyder, D. E. (1993), "Capturing multiple perspectives: A user-centered approach to knowledge acquisition", *Knowledge Acquisition*, *5* (1), 79-116

# Appendix: Y6 Full Publication List

MURI: Computer-aided Human-Centric Cyber Situation Awareness

PI: Peng Liu

**Papers published in or under review by peer-reviewed journals**

1. E. Serra, S. Jajodia, A. Pugliese, A. Rullo, and V.S. Subrahmanian. Pareto-Optimal Adversarial Defense of Enterprise Systems, ACM Transactions on Information & Systems Security, 17(3): 11:1-11:39 (2015).
2. L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, "Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks," Submitted to IEEE Transactions on Information Forensics & Security, 2015.
3. Ben-Asher, N. & Gonzalez C. (2015). Effects of Cyber Security Knowledge on Attack Detection. *Computers in Human Behavior*. 48: 51-61.
4. A. Azaria, A. Richardson, S. Kraus and V.S. Subrahmanian. Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data, IEEE Transactions on Computational Social Systems, 1.2 (2014): 135-155, November 2014.
5. Yoon-Chan Jhi, Xinran Wang, Xiaoqi Jia, Sencun Zhu, Peng Liu, and Dinghao Wu, "Program Characterization Using Runtime Values and Its Application to Software Plagiarism Detection," IEEE Transactions on Software Engineering, accepted, to appear, 2016
6. Jiang Ming, Fangfang Zhang, Dinghao Wu, Peng Liu, and Sencun Zhu, "Deviation-Based Obfuscation-Resilient Program Equivalence Checking with Application to Software Plagiarism Detection," IEEE Transactions on Reliability, 2016, under Minor revision
7. Q. Zeng, J. Rhee, H. Zhang, N. Arora, G. Jiang, P. Liu, "Precise and and Scalable Calling Context Encoding," submitted to ACM Transactions on Software Engineering and Methodology, 2016
8. C. Zhong, J. Yen, P. Liu, R. F. Erbacher, Learn from Analysts' Working Experience: Towards Automated Cybersecurity Data Triage, submitted to IEEE Transactions on Human Machine Systems, 2016

**Presentations at meetings, but not published in Conference Proceedings**

1. V.S. Subrahmanian, Invited Speaker, Israel National Cyber-Security Conference, June 2015.
2. V.S. Subrahmanian, Invited Speaker, Summer School on Business Intelligence and Big Data Analysis, Capri, Italy, June 2015.
3. V.S. Subrahmanian, Invited Speaker, Cyber-Security and Resilience Conference, Bombay Stock Exchange, Mumbai, India, April 2015.
4. V.S. Subrahmanian, Invited Participant, India-Israel Dialog, New Delhi, Dec 2014.
5. V.S. Subrahmanian, Invited Speaker, 4th Annual International Cybersecurity Conference, Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University, the Israeli

National Cyber Bureau, Prime Minister Office and the Interdisciplinary Cyber Research Center (ICRC), Sep 2014.

6. V.S. Subrahmanian, Commencement/Graduation Speaker, PES Institute of Technology, Bangalore, India, Sep 2014.
7. Cooke, N. J., Shope, S. M., Bradbury, A., & Champion, M. (2014). DEXTAR: A Cyber Security Testbed. ASU's Symposium on Information Assurance Research and Education, October 16, 2014, Tempe, AZ

**Peer-Reviewed Conference Proceeding publications (other than abstracts)**

1. R. Wang, W. Enck, D. Reeves, X. Zhang, P. Ning, D. Xu, W. Zhou, and A. Azab, "EASEAndroid: Automatic Policy Analysis and Refinement for Security Enchanced Android via Large-Scale Semi-Supervised Learning", In Proc. of the 24th USENIX Security Symposium (August 2015, Washington DC), 2015, published.
2. Chuangang Ren, Yulong Zhang, Hui Xue, Tao Wei, Peng Liu, "Towards Discovering and Understanding Task Hijacking in Android," USENIX Security 2015, published.
3. Jiang Ming, Dinghao Wu, Gaoyao Xiao, Jun Wang, and Peng Liu, "TaintPipe: Pipelined Symbolic Taint Analysis," USENIX Security 2015, published
4. Kai Chen, Peng Wang, Yeonjoon Lee, Xiaofeng Wang, Nan Zhang, Heqing Huang, Wei Zou, Peng Liu, "Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale," USENIX Security 2015, published.
5. Mingyi Zhao, Jens Grossklags, Peng Liu, "An Empirical Study of Web Vulnerability Discovery Ecosystems," ACM CCS 2015, published.
6. C. Zhong, J. Yen, P. Liu, R. Erbacher, R. Etoty, and C. Garneau, "An Integrated Computer-Aided Cognitive Task Analysis Method for Tracing Cyber-Attack Analysis Processes," Proceedings of the 2015 Symposium and Bootcamp on the Science of Security, ACM, 2015, published.
7. Q. Zeng, M. Zhao, P. Liu, "HeapTherapy: An Efficient End-to-end Solution against Heap Buffer Overflows," DSN 2015, published.
8. B. Zhao, P. Liu, "Private Browsing Mode Not Really That Private: Dealing with Privacy Breach Caused by Browser Extensions," DSN 2015, published.
9. Jun Wang, Mingyi Zhao, Qiang Zeng, Dinghao Wu, and Peng Liu, "Risk Assessment of Buffer 'Heartbleed' Over-read Vulnerabilities" (Practical Experience Report), In Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2015), Rio de Janeiro, Brazil, June 22-25, 2015. (Published).

**10.** Heqing Huang, Kai Chen, Chuangang Ren, Peng Liu, Sencun Zhu and Dinghao Wu, "Towards Discovering and Understanding the Unexpected Hazards in Tailoring Antivirus Software for Android," ACM ASIACCS 2015, full paper, published.

**11.** Jun Wang, Zhiyun Qian, Zhichun Li, Zhenyu Wu, Junghwan Rhee, Xia Ning, Peng Liu and Geoff Jiang, "Discover and Tame Long-running Idling Processes in Enterprise Systems," ACM ASIACCS 2015, full paper, published.

**12.** Zhongwen Zhang, Peng Liu, Ji Xiang, Jiwu Jing and Lingguang Lei, "How Your Phone Camera Can Be Used to Stealthily Spy on You: Transplantation Attacks against Android Camera Service," ACM CODASPY 2015, published.

13. M. Albanese, E. Battista, and S. Jajodia, "A Deception Based Approach for Defeating OS and Service Fingerprinting," To appear in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), Florence, Italy, September 28-30, 2015.
14. S. Venkatesan, M. Albanese, and S. Jajodia. "Disrupting Stealthy Botnets through Strategic Placement of Detectors," To appear in Proceedings of the 3rd IEEE Conference on Communications and Network Security (IEEE CNS 2015), Florence, Italy, September 28-30, 2015.
15. Christopher G. Healey, Lihua Hao, and Steve E. Hutchinson, "Ensemble Visualization for Cyber Situation Awareness of Network Security Data", submitted to IEEE Symposium on Visualization for Cyber Security (VizSec 2015).
16. Ben-Asher, N. & Gonzalez, C. (2015). Training for the unknown: The role of feedback and similarity in detecting zero-day attacks. 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015). July 26-30. Las Vegas, NV.
17. S. Kumar, F. Spezzano, and V.S. Subrahmanian. VEWS: A Wikipedia Vandal Early Warning System, Proc. 2015 ACM KDD, August 2015, Sydney Australia
18. S. Kumar, F. Spezzano, V.S. Subrahmanian. Accurately Detecting Trolls in Slashdot Zoo via Decluttering, Proc. ACM/IEEE Intl. Conf. on Advances in Social Network Analysis and Mining (ASONAM) 2014, Beijing, August 2014.
19. McNeese, M. D., Mancuso, V. F., McNeese, N. J., & Glantz, E. (2015), "What went wrong? What can go right? A prospectus on human factors practice", to appear in Proceedings of the 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE, July, 2015, Las Vegas, NV
20. Hall, D., McMullen, S. and C.M. Hall (2015), "New perspectives on Level-5 information fusion: The impact of advances in information technology and user behavior," accepted for the IEEE 2015 International Conference on Multisensor Fusion and Integration for Intelligent Systems, Sept. 14 – 16, 2015, San Diego, CA.
21. Hall, D. L., J. Graham and E. Catherman, (2015), "A survey of tools for the next generation analyst", Proceedings of the DSS Sensing Technology and Applications Analyst: Next-Generation Analyst III, 20-24 April, 2015, Baltimore, MD

22. Xiaoyan Sun, Anoop Singhal, Peng Liu, "Who Touched My Mission: Towards Probabilistic Mission Impact Assessment," In Proceedings of ACM SafeConfig Workshop, in association with ACM CCS 2015.
23. Champion, M., Jariwala, S. Ward, P., & Cooke, N. J. (2014). Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. Proceedings of the 57th Annual Conference of the Human Factors and Ergonomics Society, Santa Monica, CA: Human Factors and Ergonomics Society.
24. Ben-Asher, N., Rajivan, P., Cooke, N., & Gonzalez, C. (2014). Studying the dynamics of cyber-war through instance-based learning and multi-agent modeling. Proceedings of the 4th Midwestern Cognitive Science Conference, Dayton, OH, p. 34.

**Book Chapters**

1. Gonzalez, C.; Ben-Asher, N.; Oltramari, A.; Lebiere, C. (In press). Cognitive Models of Cyber Situation Awareness and Decision Making. In C. Wang, A. Kott, & R. Erbacher (eds.), Cyber defense and situational awareness.
2. D., and D. L. Hall, D., G. Cai and J. Graham (2015, in press), "Empowering the next generation analyst" chapter in *Information Fusion in Crisis Management*, ed. By G. Ragova and P. Scott, Springer.
3. M. Albanese and S. Jajodia, "Technological Solutions for Improving Cyber Security Performance," To appear in *The Psychosocial Dynamics of Cyber Security*, Springer, 2015.
4. Rajivan, P., & Cooke, N. J., "On the Impact of Team Collaboration on Cyber SA," In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
5. Sushil Jajodia and Massimiliano Albanese, An Integrated Framework for Cyber Situational Awareness, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
6. Christopher G. Healey, Lihua Hao, and Steve E. Hutchinson, Lessons Learned: Visualizing Cyber Situation Awareness in a Network Security Domain, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
7. X. Sun, J. Dai, A. Singhal, P. Liu, Enterprise-level Cyber Situation Awareness, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
8. Cleotilde Gonzalez, Noam Ben-Asher, Don Morrison, Dynamics of Decision Making in Cyber Defense: Using Multi-Agent Cognitive Modeling to Understand CyberWar, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
9. Chen Zhong, John Yen, Peng Liu, Rob Erbacher, Christopher Garneau, Studying Analysts Data Triage Operations in Cyber Defense Situational Analysis, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming
10. Michael D. McNeese, David L. Hall, The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems, In P. Liu, S. Jajodia, and C. Wang (Eds.), Recent Advances in Cyber Situation Awareness, Springer, 2016, forthcoming

**Books**

- S. Jajodia, P. Shakarian, V.S. Subrahmanian, V. Swarup, C. Wang (eds). Cyber-Warfare: Building the Scientific Foundation, Springer 2015.

**Other – Dissertations & Theses**

1. Lihua Hao, "Octree and Clustering Based Hierarchical Ensemble Visualization," Ph.D. dissertation, December 2014, North Carolina State University.

2. Rajivan, P. (2015). Information Pooling Bias in Collaborative Cyber Forensics. PhD dissertation, Arizona State University.

3. Jun Wang, PROTECTING SERVER PROGRAMS AND SYSTEMS: PRIVILEGE SEPARATION, ATTACK SURFACE REDUCTION, AND RISK ASSESSMENT, PhD Dissertation, College of IST, November 2015, Penn State University.

4. Bin Zhao, IDENTIFYING PRIVATE DATA LEAKAGE THREATS IN WEB BROWSERS, PhD Dissertation, College of IST, June 2015, Penn State University.

5. Qiang Zeng, "IMPROVING SOFTWARE SECURITY WITH CONCURRENT MONITORING, AUTOMATED DIAGNOSIS, AND SELF-SHIELDING," PhD Dissertation, Dept. of CSE, College of Engineering, Penn State University, Oct. 2014

6. Gaoyao Xiao, DETECTING AUTOMATED AGENTS BASED INSIDER ATTACKS THROUGH ADJACENCY MATRIX ANALYSIS, MS Thesis, College of IST, Spring 2015, Penn State University

**Other – Editorial Preface:** None